



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JANNE MANKINEN

Mobiilimaksamisen ratkaisuja Suomessa

Diplomityö

Tarkastaja: Yliopistonlehtori Timo Aaltonen
Tarkastaja ja aihe hyväksytty Tieto- ja
sähkötekniikan tiedekuntaneuvoston
kokouksessa 28. helmikuuta 2018

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan diplomi-insinöörin tutkinto-ohjelma

JANNE MANKINEN: *Mobiilimaksamisen ratkaisuja Suomessa*

Diplomityö, 49 sivua

Toukokuu 2018

Pääaine: *Ohjelmistotuotanto*

Tarkastaja: Yliopistonlehtori *Timo Aaltonen*

Avainsanat: mobiilimaksaminen, maksupalvelu, mobiilisovellus, mobiili, vertailu, Suomi

2000-luvun alussa Suomessa tapahtunut korttimaksamisen murros loi vahvan pohjan myös muille sähköisille maksutavoille, kuten mobiilimaksamiselle. Mobiilimaksaminen on nopeasti yleistynyt maksutapa, jossa maksusta vähintään yksi osasuoritus on toteutettu mobiililaitteella. Mobiilimaksaminen voidaan toteuttaa useilla erilaisilla tavoilla. Nämä tavat soveltuvat erilaisiin tilanteisiin eri tavoin, sillä jokaisella valinnalla on omat hyvät ja huonot puolensa. Tällöin on haastavaa päättää, mitä ratkaisua halutaan lähteä kehittämään ja miksi se soveltuisi tarpeeseen muita paremmin.

Suomessa käytössä olevat mobiilimaksamisen ratkaisut voidaan karkeasti jakaa kolmeen erilaiseen lähestymistapaan. Yksi tapa on toteuttaa kokonaan oma järjestelmä, jossa maksuja käsitellään yksilöllisillä tunnisteilla eli tokeneilla. Toinen tapa on hyödyntää mobiililaitteista löytyvää NFC-yhteyttä sekä nykyään useimmista maksupääätteistä löytyvää lähimaksuominaisuutta. Kolmas tapa on luottaa mobiilimaksuratkaisunsa ulkopuolisen palvelun tarjoajan käsiin.

Tässä diplomityössä esitellään ja vertaillaan näitä Suomessa käytössä olevaa kolmea teknologiaratkaisua keskenään. Työn tarkoituksena on auttaa lukijaa ymmärtämään mobiilimaksamisen pääpiirteitä sekä eri ratkaisujen ominaisuuksia, joiden avulla on mahdollista valita omaan tarpeeseen parhaiten soveltuva ratkaisu. Vertailussa käydään läpi eri ratkaisujen kehitys- ja käyttökustannuksia sekä räätälöintimahdollisuuksia. Vertailtavat ominaisuudet ovat mobiilimaksupalvelun offline-käyttömahdollisuus, yhteensopivat maksupaikat, tuetut mobiililaitteet sekä käyttäjien seurantamahdollisuudet.

Omaan tarpeeseen sopivan yhtälön löytäminen voi olla työlästä, eikä jokaiseen tapaukseen löydy yhtä yksittäistä vastausta. Vaihtuvien olosuhteiden vuoksi onkin mahdotonta sanoa, mikä esitellyistä ratkaisuista on paras kaikissa tilanteissa. Sopivimman ratkaisun saavuttaminen vaatii täten aina oman todellisen tarpeen selvittämistä ja esiteltyjen vaihtoehtojen punnitsemista näistä lähtökohdista. Työssä pyritään tarjoamaan ratkaisujen vertailuun mahdollisimman hyvät työkalut.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY

Master's Degree Program in *Pervasive Computing*

JANNE MANKINEN: *Mobile Payment Solutions in Finland*

Master of Science in Technology Thesis, 49 pages

May 2018

Major: *Software Engineering*

Examiner: University Lecturer *Timo Aaltonen*

Keywords: mobile payment, payment service, mobile application, mobile, comparison, Finland

Card payment services turning point in the early 21st century created a strong foundation for other electrical payment methods, such as mobile payments, in Finland. Mobile payments are a fast growing payment method where at least one part of the payment execution is performed with a mobile device. Mobile payments can be achieved with multiple different solutions. Each of these solutions perform differently on every situation, since all of them have their own pros and cons. That is why it is so hard to decide which solution is the one to be developed and why that would apply better than the others.

The mobile payment solutions used in Finland can be divided into three separated approaches. One of them is to develop entire service where the payments are performed with unique tokens. The second way to approach this is to use mobile devices' NFC-connection and contactless payment abilities of the most modern payment terminals. The third way is to make an agreement of usage with separate service provider.

This thesis introduces and compares together these three technology solutions used in Finland. The intention of this thesis is help the reader understanding the main outlines of mobile payments and attributes of each solution. This makes it possible to consider all options and select the best suiting solution for the reader's own need. The comparison includes different development and operating expenses as well as customizing opportunities. Compared customizations are offline usage possibilities, compatible business places, supported mobile devices and also user action monitoring.

It can be hard to find a suitable solution for own demands and there is no one correct application for every need. Changing conditions makes it impossible to say which solution is the best for all the situations. Finding the most favourable solution always needs examining the actual necessities and comparing the solutions from this basis. This thesis intends to offer as good tools as possible for this comparison.

ALKUSANAT

Kiitän professori Petri Ihantolaa, joka avusti tämän diplomityön aloittamisessa ja työni lopullista tarkastajaa yliopistonlehtori Timo Aaltosta, joka auttoi minua viemään tämän työn viimein maaliin. Lisäksi kiitän ohjaajaani ja esimiestäni Esa Lähteenmäkeä kaikesta tuesta, ideoista ja kannustuksesta, joita olen saanut työn aikana. Haluan kiittää myös työnantajaani Eatech Oy:tä joustavuudesta, joka mahdollisti opintojeni viimeistelyn töiden ohella.

Suuret kiitokset kuuluvat myös rakkaalle tyttöystävälleni Senjalle kaikesta kannustuksesta ja kielellisestä tuesta, jota hän siinä minua lahjakkaampana antoi. Lisäksi haluan kiittää rakkaita vanhempiani tärkeästä tuesta koko opintojeni aikana sekä molempia isoveljiäni, jotka esimerkillään ja toisaalta haastamisellaan auttoivat sekä valitsemaan että kulkemaan omaa tietäni.

Tampere, 18. toukokuuta 2018

Janne Mankinen

SISÄLLYSLUETTELO

1. Johdanto	1
2. Johdatus mobiilimaksamiseen	3
2.1 Korttimaksaminen	3
2.1.1 Maksun elinkaari	4
2.1.2 Erilaiset maksukortit ja lähimaksaminen	5
2.2 Mobiilimaksaminen	7
2.2.1 Mobiilimaksamiselle asetettuja vaatimuksia ja toiveita	7
2.2.2 Mobiilisovellusten haasteet	9
3. Mobiilimaksamisen ratkaisuja	11
3.1 Token-pohjaiset ratkaisut	12
3.1.1 Perusidea	12
3.1.2 Vaatimukset ja haasteet	16
3.1.3 Mahdollisuudet	17
3.2 Fyysinen kortti emuloituna, HCE	18
3.2.1 Perustiedot	18
3.2.2 Käyttöönotto	21
3.2.3 Vaatimuksia ja haasteita	25
3.3 Virtuaalinen maksukortti	27
3.3.1 Perustiedot	27
3.3.2 Käyttöönotto	28
3.3.3 Vaatimukset	28
4. Vertailu	30
4.1 Kehityskustannukset	30
4.2 Käyttökustannukset	31
4.2.1 Kustannuksien yhteenveto	34
4.3 Räätelöitävyys	35
4.3.1 Offline-käyttö	35
4.3.2 Maksupaikat	36
4.3.3 Laitetuki	37
4.3.4 Käyttäjien seuranta	37
4.3.5 Ominaisuuksien yhteenveto	38
4.4 Mobiilimaksamisen tulevaisuus	40
5. Yhteenveto	42
Viitteet	44

KUVALUETTELO

Kuva 1.	<i>Korttimaksu on nopeasti noussut käteistä suositummaksi maksutavaksi päivittäistavaraostoissa. [7]</i>	4
Kuva 2.	<i>Maksun elinkaari kahden pankin välisessä maksussa.</i>	5
Kuva 3.	<i>Yksi tapa mobiilimaksamisessa käytetyistä tiedonsiirroista. Katkoviiva ilmaisee vapaavalintaisen tiedonsiirron. Vihreällä värillä on korostettu yhtäaikainen tiedonsiirto.</i>	13
Kuva 4.	<i>Toinen tapa mobiilimaksamisessa käytetyistä tiedonsiirroista, jossa kassapääte hoitaa tietojen välittämisen. Katkoviivat ilmaisevat vapaavalintaisen tiedonsiirron.</i>	14
Kuva 5.	<i>Kolmas tapa mobiilimaksamisessa käytetyistä tiedonsiirroista, jossa mobiililaite ja kassapääte eivät suoraan vaihda keskenään tietoa.</i>	15
Kuva 6.	<i>Mobiililaitteen NFC-piiri hakee maksukortin tiedot suoraan Secure Elementiltä.</i>	19
Kuva 7.	<i>Mobiililaitteen NFC-piiri hakee maksukortin tiedot prosessorilta, joka saa ne suoritettavalta sovellukselta.</i>	19
Kuva 8.	<i>NFC-ohjaimen ennalta määrätty lista kertoo, mistä tiedot haetaan kyseisellä AID:llä.</i>	20
Kuva 9.	<i>Eri ratkaisujen kokonaiskustannusarviot.</i>	34

TAULUKKOLUETTELO

<i>Taulukko 1.</i>	<i>Arvioudut kokonaiskustannukset erilaisten käyttötarpeiden mukaan Debit-korteilla. Summat ovat euroina.</i>	<i>32</i>
<i>Taulukko 2.</i>	<i>Arvioudut kokonaiskustannukset erilaisten käyttötarpeiden mukaan Credit-korteilla. Summat ovat euroina.</i>	<i>33</i>
<i>Taulukko 3.</i>	<i>Ominaisuuksien vertailu eri ratkaisujen välillä. Tähtien asteikko on yhdestä viiteen tähteä.</i>	<i>39</i>

OHJELMALUETTELO

1	Select AID APDU -viestin sisältö [50, 46].	21
2	Select AID APDU -viestin vastaus, jossa valitaan käytettäväksi Visa Credit- tai Debit-kortti [50, 46]. Viestin sisältö on sisennetty lohkoittain.	22
3	Oma maksupalveluluokka MyPaymentService, joka laajentaa Androidin HostApduService-luokkaa ja ylikirjoittaa processCommandApdu-funktion [49].	23
4	Maksupalvelun lisääminen Android Manifestiin. [49]	23
5	Tuettujen Application ID:iden lista. [49]	24

KIRJAINLYHENTEET JA TERMIT

KIRJAINLYHENTEET

AID	Application Identifier
APDU	Application Protocol Data Unit
EMV	Europay - MasterCard - Visa
GDPR	General Data Protection Regulation
GPO	Get Processing Options
HCE	Host Card Emulation
NFC	Near Field Communication
PIN	Personal Identification Number
PPSE	Proximity Payment System Environment
PSD2	Payment Services Directive 2
QR	Quick Response
SE	Secure Element

TERMIT

Termi	Selitys
AID	EMV-ympäristössä maksukorttityypin tunniste
Android Manifest	Android-sovelluksen määrittelytiedosto, jossa ilmoitetaan mitä oikeuksia ja ominaisuuksia sovellus vaatii, ja määritellään sovelluksen kaikkien näkymien tiedot.
Application Protocol Data Unit	Standardin ISO/IEC 7816-4 mukainen tietopaketti, joka voi pitää sisällään maksukortin organisaation ja tyypin.
Autentikointi	Käyttäjän tai henkilön identiteetin varmentaminen. Voidaan suorittaa esimerkiksi salasanalla, Pin-koodilla tai sormenjälkitunnistuksella.
Credit-kortti	Luottokortti, jonka ostot peritään luottoyhtiöltä, joka laskuttaa kortinhaltijaa myöhemmin sopimuksensa mukaisesti.
Debit-kortti	Pankkikortti, jolla voidaan maksaa ostoksia sekä nostaa rahaa pankkiautomaateista. Tällöin raha veloitetaan katevarmennuksen avulla pankkitililtä.
Emuloiminen	Toiminto, jossa jäljitellään toisen järjestelmän toimintaa.
EMV	Standardoitu protokolla maksukorteille, joka korvasi magneettijuovan turvallisempaa vaihtoehtona. Suomessa pakollinen vuodesta 2005 alkaen.
Etämaksu	Maksaminen ilman fyysistä kontaktia maksupäätteen kanssa. Esimerkiksi maksaminen verkkopankissa tai mobiilisovelluksella.
Host Card Emulation	Android-käyttöjärjestelmän ominaisuus, joka mahdollistaa maksukortin emuloimisen mobiilisovelluksessa. Esitelty Android 4.4 -versiossa.
Katevarmennus	Debit-kortilla maksettaessa tapahtuva varaus pankkitililtä, joka tilitetään varmennuksen mukaisesti. Tällä voidaan estää tilin ylitys, eli rahavarojen käyttäminen yli tilin saldon.
Kortinhaltija	Henkilökohtaisen maksukortin omistava henkilö.
Lähimaksaminen	Maksukortilla tai mobiililaitteella maksaminen viemällä ne lähelle lähimaksua tukevaa maksupäätettä.
Magneettijuova	Maksukortissa oleva magneettinen alue, jolle on talletettu maksukortin tietoja. Otettu käyttöön 1960-luvulla, eikä sisällä kovin hyvää suojausta.
Maksupääte	Laite, joka mahdollistaa maksutapahtuman varmentamisen asiakkaan ja kauppiaan välillä.
Mobiililaitte	Laite, joka on suunniteltu kuljetettavaksi mukana ja kykenee käsittelemään paikallista tietoa sekä tukee yleensä myös langatonta tiedonsiirtoa.
Mobiilimaksu	Maksu, josta vähintään yksi osasuoritus on suoritettu mobiililaitteella.

Termi	Selitys
Offline-käyttö	Ilman internet-yhteyttä tapahtuva mobiilisovelluksen tai -laitteen käyttäminen.
Ohjelmointikieli	Formaali kieli, jota käytetään tietokoneen ymmärtämien toimintaohjeiden antamiseen.
Pin-koodi	Tunnusluku, jota käytetään tunnistautumiseen. Usein maksukorteissa neljä numeroa pitkä.
QR-koodi	Kaksiulotteinen viivakoodi, johon voidaan sisällyttää dataa sekä pysty- että vaakasuuntaan.
Secure Element	Joistakin Android-mobiililaitteista löytyvä erillinen tietoturvallinen säiliö, johon on voitu tallentaa esimerkiksi maksukortin tietoja.
Token	Järjestelmässä yleensä ainutlaatuinen kirjain-numero-yhdistelmä, jota voidaan käyttää esimerkiksi autentikointiin.
Tunnistautuminen	Katso <i>Autentikointi</i>

1. JOHDANTO

Mobiilimaksaminen on yleistynyt räjähdysmäisesti kuluneiden muutaman vuoden aikana [1]. Useat pankit ovat kehittäneet oman mobiilimaksujärjestelmän muiden tuotteidensa ja palveluidensa tueksi. Myös monet muut tahot ovat kehittäneet omia mobiilimaksuratkaisujaan, kuten mobiilitankkausta huoltoasemille [2, 3]. Mobiilimaksamista markkinoidaan modernina tapana sekä käteisen että perinteisten maksukorttien korvaajaksi painottaen nopeutta ja helppoutta verrattuna perinteisiin maksutapoihin. Tällöin käyttäjän ei tarvitse kuljettaa mukanaan muuta kuin omaa mobiililaitettaan.

Mobiilimaksamisen toteuttamiseen on useita erilaisia lähestymistapoja. Osa ratkaisuksista vaatii käyttäjän mobiililaitteelta tiettyjä ominaisuuksia, kuten NFC-sirua [4], toisissa vaihtoehdoissa riittää pelkkä internet-yhteys ja jotkin ratkaisut hyödyntävät laitteen kameraa maksun tiedoista muodostetun viivakoodin lukemiseksi. Tässä työssä esitellään yleisiä mobiilimaksamisen piirteitä ja ominaisuuksia, sekä esitellään yleisimpiä mobiilimaksamisen mahdollistavia tekniikoita ja vertaillaan niiden mahdollisuuksia ja rajoituksia. Esiteltyjen seikkojen avulla lukijan on mahdollista punnita omaan tilanteeseensa parhaiten soveltuva ratkaisu. Työ tarjoaa myös neuvoja ratkaisujen käyttöönottamiseksi. Lisäksi pohditaan mobiilimaksamisen tulevaisuutta sekä mahdollisia käyttötapauksia.

Tämä työ on tarkoitettu maksukortin mobiilimaksamisen käyttöönottoa suunnittelevalle, riippumatta siitä, onko lukija tilaajan roolissa vai järjestelmän toteuttavana osapuolena. Lukijan oletetaan ymmärtävän perusasioita ohjelmistojen tuottamisesta, sekä mobiilikäyttöjärjestelmistä ja -ympäristöistä. Lukijan oletetaan tuntevan myös maksamiseen liittyviä käytäntöjä ja toimintatapoja.

Työssä aihetta lähestytään ensisijaisesti mobiililaitteiden näkökulmasta, jolloin tarkat kuvaukset esimerkiksi pankkitoimintojen ja sovellusten taustajärjestelmistä rajataan pois. Tämän lisäksi työssä keskitytään pääasiallisesti Android- ja iOS-mobiilialustoihin, sillä ne ovat kirjoitushetkellä ehdottomasti suosituimmat mobiilialustat [5]. Työstä rajataan pois myös tarkempi paneutuminen tietoturvaan ja sen toteuttamistapoihin mobiilimaksujärjestelmissä. Käsittelyssä keskitytään lähinnä mobiilimaksamisen tilanteeseen Suomessa.

Mobiilimaksaminen on monipuolinen käsite, ja se määritellään tarkemmin luvussa 2. Lisäksi luvussa kerrotaan lyhyesti erilaisista maksukorteista sekä yleistä tietoa maksukorttijärjestelmistä. Luvussa 3 esitellään erilaisia lähestymistapoja mobiilimaksamisen toteuttamiseen. Ensimmäisenä käsitellään erilaisia token-pohjaisia ratkaisuja, jotka tarkoittavat mobiililaitteen ja palvelimen viestien välittämiseen perustuvaa maksun varmennusta. Tämän jälkeen esitellään fyysisen maksukortin emuloimista mobiililaitteella sekä lopuksi ulkopuolisten palveluntarjoajien ja mobiililaittevalmistajien tarjoamia ratkaisuja mobiili-

maksamisen käyttöönottamiseksi. Luvussa 4 eri teknologiaratkaisuja vertaillaan keskenään kehitys- ja käyttökustannusten sekä räätälöintimahdollisuuksien mukaan. Lisäksi punnitaan yksilöllisesti eri ratkaisujen etuja ja rajoituksia, sekä pohditaan tulevaisuudennäkymiä mobiilimaksamisen osalta. Viimeisessä luvussa on tämän työn yhteenveto.

2. JOHDATUS MOBIILIMAKSAMISEEN

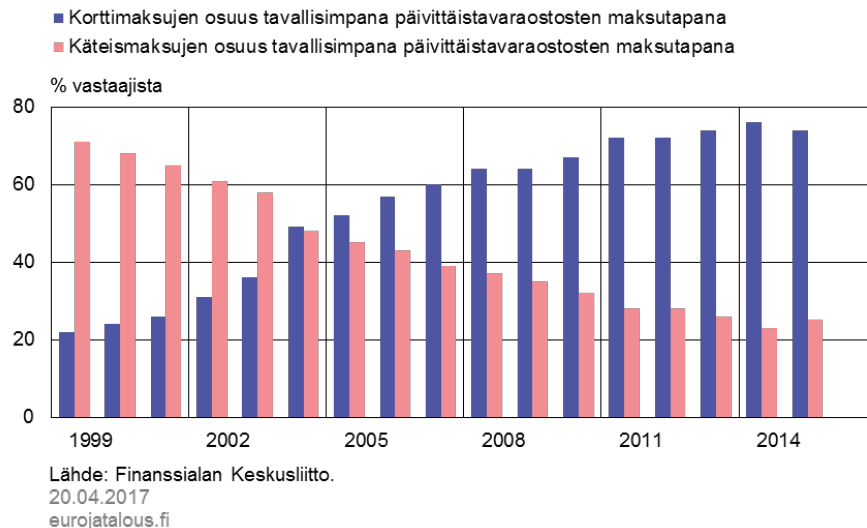
Tässä luvussa kerrotaan tarkemmin yleisiä piirteitä korttimaksamisesta, maksujen suorittamisesta, mobiilimaksamisesta sekä siihen liittyvistä järjestelmistä. Tämän lisäksi lukijalle annetaan tarpeelliset perustiedot erilaisista maksukorteista ja mobiilisovellusten haasteista. Luvussa esiteltyjen tietojen avulla on tarkoitus valmistaa lukijaa tarvittavissa määrin seuraavassa luvussa käsiteltäviin mobiilimaksamisen ratkaisuihin ja niiden ominaispiirteisiin.

2.1 Korttimaksaminen

Korttimaksamisella tarkoitetaan tavallista pankki- tai luottokortilla maksamista. Maksu suoritetaan *maksupäätteen* avulla. Maksupääte on korttimaksamisen mahdollistava laite, jonka avulla *varmennetaan* ja suoritetaan maksuja asiakkaan ja kauppiaan välillä sähköisesti. Varmentaminen eli *kortinhaltijan* tunnistautuminen voidaan toteuttaa esimerkiksi nelinumeroisella *pin-koodilla* eli tunnusluvulla, joka asiakasta pyydetään syöttämään maksupäätteelle maksun hyväksymiseksi.

Korttimaksun tapauksessa pankit hoitavat sähköisesti maksun käsittelyn sekä valuutan siirtämisen tililtä toiselle tarvittaessa pankkien välillä. Tämä mahdollistaa nopean ja vaivattoman sekä turvallisen maksamisen etenkin Suomessa, joka onkin muiden Pohjoismaiden lisäksi yksi maailman johtavia korttimaksamisen maita [6]. Tämä näkyy korkeassa käyttöprosentissa sekä siinä, kuinka korttimaksaminen on mahdollista lähes kaikissa kaupoissa.

Suomessa ensimmäiset maksupäätteet otettiin julkiseen käyttöön 1980-luvun puolivälissä, ensin huoltoasemilla ja niiden jälkeen myös kaupoissa. Korttimaksaminen kehittyi ja yleistyi aluksi hitaasti, mutta teknologian yleisen kehittymisen myötä myös maksutavat edistyivät ja korttimaksaminen ohitti käteisen käytön täpärästi jo vuonna 2004 [7]. Ehdottomasti suurin osa Suomessa tapahtuvista päivittäistavaraostoista suoritetaan nykyään maksukortilla. Tämä voidaan havaita myös kuvasta 1, joka osoittaa lisäksi maksamisen nopean murroksen ja korttimaksamisen yleistymisen 2000-luvun alussa.



Kuva 1. Korttimaksu on nopeasti noussut käteistä suosituimmaksi maksutavaksi päivittäistavaraostoissa. [7]

Korttimaksamisen yleistymisen ei kuitenkaan ole aivan ongelmattonta, sillä sen käyttämisestä koituvat kustannukset voivat olla kauppiaille merkittävä menoerä muiden kulujen lisäksi. Yle Uutisten haastattelussa Suomen Yrittäjien lainopillinen asiamies Atte Rytönen toteaa näiden kulujen olevan seitsemästä sentistä aina kahdeksaankymmeneen senttiin maksua kohden [8, 9]. Summa riippuu oston suuruudesta, ja yritys voi halutessaan itse periä kuluttajilta vieläkin korkeampaa summaa korttimaksusta. Tämä menoerä kuitenkin yleensä sisällytetään korkeampiin hintoihin, ja täten se päättyy kuluttajien maksettavaksi, kuten kaikki muutkin kaupan kustannukset, jotta liiketoiminta olisi kannattavaa.

Toinen ongelma korttimaksamisessa on ns. *skimmaus-laitteet*, eli laitteet, joilla rikolliset pyrkivät kopioimaan maksukortteja omiin tarkoituksiinsa. Skimmaus-laite kiinnitetään yleensä maksuautomaattiin, jossa sillä pyritään lukemaan syötetyn maksukortin magneettijuova, jonka tietojen avulla maksuja voidaan suorittaa. Suomessa poliisin järjestelmiin kirjattiin 81 kappaletta epäiltyjä skimmaus-tapauksia vuonna 2016. [10] Magneettijuova on otettu käyttöön jo 1960-luvulla, eikä niissä täten ole yhtä hyvää suojausta kuin uudempien maksukorttien EMV-siruissa. Tämä suojauksen puute mahdollistaa magneettijuovalle tallennettujen tietojen helpomman kopioimisen.

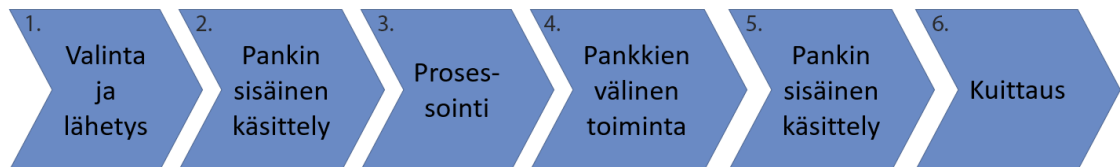
2.1.1 Maksun elinkaari

Seuraavaksi käydään vaihe vaiheelta läpi, kuinka korttimaksaminen oikeastaan toimii. Maksu aloitetaan maksupäätteellä, jonka jälkeen suoritetaan seuraavat toimenpiteet [11].

1. *Valinta ja lähetys:* Ensin maksupäätte valitsee käyttäjän syöttämän kortin mukaan sopivan maksutavan ja välittää maksun tiedot kortinhaltijan pankille.

2. *Pankin sisäinen käsittely*: Pankki autentikoi eli tunnistaa kortin ja varmentaa, että maksu on laillinen ja teknisesti oikea, sekä kortista riippuen tarkistaa kortin käyttövaran.
3. *Prosessointi*: Tämän jälkeen pankki käsittelee maksun tiedot ja muotoilee tarpeellisen informaation lähetettäväksi toiselle pankille.
4. *Pankkien välinen toiminta*: Maksu siirretään pankkien välistä yhteyttä pitkin toiselle pankille käsiteltäväksi. Tässäkin vaiheessa voidaan suorittaa tarkistuksia maksun oikeellisuudesta.
5. *Pankin sisäinen käsittely*: Toinen pankki ottaa tiedon vastaan ja käsittelee maksun saajan tilille oikean summan.
6. *Kuittaus*: Lopuksi toinen pankki lähettää kuittauksen maksun onnistumisesta, joka välitetään ensimmäisen pankin kautta alkuperäiselle maksajalle maksupäätteelle.

Kuvassa 2 esitetään yllä kerrottu Euroopan keskuspankin tietojen mukainen korttimaksun elinkaari, jossa maksu tapahtuu kahden eri pankin välillä. Saman pankin sisällä tapahtuvassa maksussa esitetyt vaiheet 4 ja 5 jäävät luonnollisesti pois. Eri pankeilla voi myös olla erilaisia sisäisiä ratkaisuja, mutta joka tapauksessa rakenne on suurin piirtein sama. [11]



Kuva 2. Maksun elinkaari kahden pankin välisessä maksussa.

Tiedon kuljettamiseen hyödynnetään yleensä tavallista internet-yhteyttä. Useimmat maksupäätteet on kytketty verkkoon joko puhelinverkon avulla tai kytkemällä ne kassapäätteen verkkoyhteyteen.

2.1.2 Erilaiset maksukortit ja lähimaksaminen

Maksukortteja on monia erilaisia. Tärkeimmät maksukorttityypit ovat luottokortti eli credit-kortti, pankkikortti eli debit-kortti ja prepaid-kortti. Näistä luotto- ja pankkikortit ovat selkeästi yleisimmät korttimuodot ja samalla yleisimmät maksamistavat Euroopassa. On olemassa myös luotto- ja pankkikortin yhdistelmäkortteja, jolloin maksua suorittaessa valitaan kumpaa maksutapaa käytetään. Prepaid-korteille voidaan tallettaa haluttu summa, joka on käytettävissä ostosten tekemiseen. [11]

Luottokortin kantava ajatus on, että maksun yhteydessä summa veloitetaan kuluttajan sijaan kortin myöntäneeltä luottoyhtiöltä, joka perii kuluttajan kanssa tekemänsä sopimuksen

mukaisesti tapahtuneet ostot laskulla esimerkiksi kuukausittain. Luottokortin avulla on mahdollista suorittaa käyttäjän kannalta turvallisempia ostoja esimerkiksi internetissä, sillä luottoyhtiö voi puolustaa käyttäjän etuja ja hyvittää maksun, mikäli tilattu tuote ei esimerkiksi koskaan saapunut. Luottokorttimaksamisen ongelmana kuitenkin on, että siinä ei seurata käyttäjän tilillä olevaa käyttövaraa, jolloin on mahdollista kuluttaa enemmän varoja kuin tilillä on katetta. [11]

Pankkikortti puolestaan on liitetty suoraan käyttäjän pankkitiliin. Pankkikortteja on kahdenlaisia: toiset veloittavat suoraan tililtä ja toiset suorittavat *katevarauksen*, joka muuttuu maksuksi muutaman päivän kuluessa. Katevaraus tarkoittaa maksukyvyn tarkistamista ja maksun summan varaamista tililtä, jolloin se ei ole enää käytössä muille maksuille. Tämän avulla voidaan estää tilin ylitys eli tilanne, jossa kulutetaan enemmän varoja kuin tilillä on saldoa. Tätä voidaan pitää sekä pankkikorttien vahvuutena että heikkoutena. Katevarauskäytännön heikkous ilmenee siinä, ettei maksuja voida suorittaa ollenkaan, mikäli tilillä ei ole saldoa. Niinpä pankkikortilla ei voida ennakoida, esimerkiksi tulossa olevaa palkkaa, sillä saldon varmistaminen estää tilin ylittämisen toisin kuin luottokortilla. [11]

Prepaid-kortti on yksinkertainen maksuratkaisu, joka on usein kauppakohtainen. Siinä kortille on talletettu tietty summa rahaa, joka voidaan käyttää ennalta määrätyissä kohteissa. Prepaid-kortilla maksettaessa maksupääte ei ole enää erikseen yhteydessä pankkiin, vaan kortin tiedot ovat yleensä kaupan omassa järjestelmässä [12]. Prepaid-korteissa on usein rajattu voimassaoloaika, jonka aikana raha täytyy käyttää, tai se jää kaupalle. Nykyään markkinoille on tullut myös pankkiin yhteydessä olevia prepaid-luottokortteja, joilla voi maksaa kaikilla maksupäätteillä [13]. Nämä toimivat kuten normaalitkin luottokortit, mutta summaa ei veloiteta laskulla jälkikäteen, vaan käytettävissä olevat varat on täytynyt siirtää kortin tilille ennen maksun suorittamista.

Nykyään korttityypistä riippumatta kortteihin tarjotaan lähimaksuominaisuuksia [14, 12]. Tämä tarkoittaa, että maksu voidaan suorittaa käyttämällä maksukorttia pelkästään maksupäätteen lähimaksupinnan lähellä ilman tarvetta syöttää kortin pin-koodia. Tästä syystä lähimaksaminen on nopeampaa kuin perinteinen korttimaksaminen. Suomessa lähimaksamisen raja ilman tunnuslukua on usein 25 euroa [15, 16, 17, 18, 19]. Yleensä tätä suuremmat maksut vaativat kortin syöttämisen maksupäätteeseen tavalliseen tapaan. Jotkin maksupäätteet mahdollistavat kuitenkin myös yli 25 euron arvoisia lähimaksuja tietyillä maksukorteilla, jolloin käyttäjä varmennetaan pin-koodilla [20, 21].

Lähimaksaminen on yleensä toteutettu NFC-teknologialla, joka mahdollistaa tiedonsiirron kahden toisiaan lähellä olevan laitteen välillä [22, 14]. Lähimaksukortteihin on upotettu NFC-siru, jonka maksupääte lukee ja suorittaa maksun saamiensa tietojen mukaisesti. Tästä on kuitenkin muodostunut lähimaksukorttien ongelma, sillä siru on aina luettavissa, jolloin sopivalla laitteella tai jopa NFC-yhteensopivalla mobiililaitteella kortti on helposti kopioitavissa esimerkiksi taskun läpi julkisessa liikenteessä [22]. Tämän jälkeen kopioidulla datalla voidaan välittömästi maksaa esimerkiksi HCE- eli *Host Card Emulation* -yhteensopivalla mobiililaitteella ilman alkuperäisen käyttäjän valtuutusta tai

pin-koodia [23]. HCE mahdollistaa fyysisen kortin mallintamisen ja maksutarkoitukseen käyttämisen [4].

2.2 Mobiilimaksaminen

Mobiilimaksaminen tarkoittaa maksun suorittamista, jossa vähintään yksi osasuoritus on toteutettu mobiililaitteella, kuten puhelimella tai tabletilla [11, 24]. Toiminnaltaan se on läheistä sukua tavalliselle korttimaksamiselle [12]. Tästä syystä maksamisen murros, jota kuvattiin kuvassa 1, on osaltaan myös valmistanut pohjaa mobiilimaksamiselle. Yleistynyt korttimaksaminen on saanut päivittäistavarakaupat uudistamaan järjestelmiään, jolloin myös mobiilimaksamiselle on ollut helpompaa kehittää tukea. Kauppalehden mukaan Suomen Pankin rahahuolto-osaston johtava neuvonantaja Kari Takala on ennustanut mobiilimaksamisen syrjäyttävän korttimaksamisen sekä nopeuttavan käteisen aseman vähenemistä, jolloin käteisestä voitaisiin luopua kokonaan [25].

Mobiilimaksaminen voidaan toteuttaa usealla erilaisella lähestymistavalla. Yleisimmin mobiilimaksaminen jaetaan *lähimaksamiseen* ja *etämaksamiseen* [12]. Lähimaksamista käsiteltiin alaluvussa 2.1.2. Tällöin kortin sijaan maksutapahtumaa varten maksupäätteelle viedään mobiililaitte. Etämaksaminen puolestaan tarkoittaa maksun suorittamista ilman fyysistä kontaktia maksupäätteeseen [11]. Etämaksuja voidaan suorittaa esimerkiksi asiakkaan verkkopankissa tai mobiilisovelluksella. Mobiililaitteella niitä suoritetaan esimerkiksi siihen tarkoitettulla mobiilisovelluksella tai hyödyntäen tekstiviestejä ja puheluita tiettyihin palvelunumeroihin. Näitä lähestymistapoja käsitellään tarkemmin luvussa 3.

Yleisimmin mobiilimaksamisen ratkaisuja tarjoaa joko finanssialan järjestö, kuten pankki, mobiilioperaattori tai laitevalmistaja. Kyseessä voi olla myös yksityinen kauppias tai jopa valtio. Jokaisella niistä on omat vahvuutensa kyseisen palvelun tarjoamiseen. Pankkien vahvuus on laaja kuluttajakunta sekä läheinen yhteys kuluttajien maksukortteihin ja pankkitileihin. Mobiilioperaattori puolestaan voi tarjota palveluita yli pankkirajojen ja tarjota mobiililaitteisiin sopivia liittymiä tai lisäpalveluita. Ensimmäiset mobiilimaksuratkaisut olivatkin nimenomaan operaattoreiden kehittämiä esimerkiksi puhelimen SIM-kortilla tilaaminen ja jälkikäteen maksaminen sekä erilaiset maksutarrat, joilla voitiin suorittaa lähimaksuja [12]. Laitevalmistaja taas voi saada asiakkaita kaikilta operaattoreilta ja pankeilta, kenellä vain on kyseisen valmistajan mobiililaitte. Yksityisen kauppiaan valtti on tietty asiakaskunta, joka voi olla sitoutunut kyseiseen kauppaan ja saada täten yksilöllisempää palvelua. Valtio puolestaan voi tarjota valtakunnallisia palveluita kaikille kansalaisilleen. [24]

2.2.1 Mobiilimaksamiselle asetettuja vaatimuksia ja toiveita

Kuluttajilla on tiettyjä odotuksia ja vaatimuksia liittyen maksamiseen ja raha-asioihin liittyviin sovelluksiin ja palveluihin [12, 24]. Osa odotuksista on yhteisiä kaikkien mobiilisovellusten välillä ja osa korostuu erityisesti mobiilimaksusovellusten kohdalla. Mobiilimak-

susovelluksen kohdalla korostuvat erityisesti tietoturva, luotettavuus ja helppokäyttöisyys. Muita tärkeitä pidettyjä seikkoja ovat maksaminen mahdollisimman monilla maksupäätteillä ja mahdollisimman monien pankkien välillä. Lisäksi tärkeitä ominaisuuksia ovat maksamisen nopeus ja tarvittaessa toimiminen myös yhdessä vanhojen maksutapojen kanssa. [24]

Näiden ohella kuluttajat toivovat mobiilimaksamiselta alhaisia käyttökustannuksia, yksilöllistä palvelua ja mahdollisuutta seurata suoritettuja maksuja reaaliajassa. Lisäksi yksityisyydestä huolissaan olevat kuluttajat toivoisivat anonyymejä maksutapahtumia, jollaisia voidaan suorittaa esimerkiksi käteisellä. Myös vapaus maksaa missä ja milloin tahansa ja millä tahansa valuutalla koetaan tärkeäksi. [24]

Kauppiaille puolestaan tärkeimpiä asioita ovat nopeammat transaktioajat ja alhaisemmat investointi- ja käyttökustannukset. Lisäksi kauppiat toivovat yhteensopivuutta vanhojen ja myös tulevien maksujärjestelmien kanssa, jotta investoitu teknologia ei jää hyödyttömäksi liian nopeasti. Tärkeiksi näkökulmiksi nousevat myös järjestelmän turvallisuus [26], maksujen seuraaminen reaaliajassa ja mahdollisuus räätälöidä palvelua tarpeen mukaan esimerkiksi erilaisilla eduilla [24]. Lisäksi maksamisen nopeutuessa kaupoilla on mahdollista palvella useampia kuluttajia samassa ajassa.

Mobiilioperaattoreita mobiilimaksamisessa sen sijaan kiinnostavat arvon lisääminen olemassa oleville palveluille sekä kuluttajien sitouttaminen omiin palveluihin. Operaattorin vaihtamisen kynnyks voi kasvaa kuluttajalle suuremmaksi, mikäli yhä useampi käytössä oleva palvelu on riippuvainen kyseisestä palveluntarjoajasta. Tämä tarjoaa myös uusia tulolähteitä sekä kasvavaa liikevaihtoa, sillä kuluttajat hyödyntävät mahdollisesti useampia palveluita tuottaen näin enemmän tuloja palveluntarjoajalle. [24]

Laitevalmistajilla on verrattain nopea väylä kuluttajille valmistamiensa laitteiden kautta, sillä kuluttajien kynnys ottaa käyttöön valmistajan tarjoamia lisäpalveluita voi olla pienempi kuin täysin irrallisen palvelun käyttöönotolle. Mobiilimaksaminen voi myös tarjota mahdollisuuden päästä uusille toimialoille ja siten tarjota uudenlaista kasvua ja liikevaihtoa. Tämä voi myös mahdollistaa uudenlaista yhteistyötä esimerkiksi pankkien ja sovelluskehittäjien kanssa. [24]

Pankeille mobiilimaksaminen tarjoaa mahdollisuuksia kohottaa brändiä sekä sitouttaa asiakkaita uusien palveluiden avulla. Tämä voi mahdollistaa myös uutta liiketoimintaa. Lisäksi pankkeja kiinnostavat turvallisuus ja erilaisten maksupetosten minimointi sekä mobiilimaksamisen integroiminen olemassa oleviin järjestelmiin. [24]

Lyhyesti tiivistettynä voidaan todeta useiden eri tahojen toivovan ja vaativan mobiilimaksamiselta lukuisia erilaisia asioita. Yhteisenä kantavana teemana voidaan kuitenkin huomata tietoturvan korostunut merkitys sekä toiveet uudenlaisesta liiketoiminnasta ja kasvavasta liikevaihdosta. Lisäksi järjestelmistä pyritään kehittämään mahdollisimman vaivattomia ja helppoja käyttää.

2.2.2 Mobiilisovellusten haasteet

Mobiilisovelluksiin liittyy omanlaisiaan haasteita, jotka vaikuttavat tästä syystä myös mobiilimaksamissovellusten kehittämiseen. Ensinnäkin erilaisia mobiililaitteita on erittäin paljon, mikä aiheuttaa erilaisia haasteita mobiilisovellusten kehittämiseen ja ylläpitämiseen [27]. Esimerkiksi pelkästään erilaisia Android-laitteita oli vuonna 2015 yhteensä 24 093 kappaletta yhteensä 1 294:ltä eri valmistajalta [28]. Kasvu on ollut lähes eksponentiaalista, joten lukumäärän voidaan olettaa kirjoitushetkellä olevan vielä merkittävästi tätäkin suurempi [28]. Tämä tarkoittaa valtavaa lukumäärää erilaisia yhdistelmiä ominaisuuksista, joita ovat esimerkiksi näytön koko, resoluutio, suorituskyky, tuetut matkapuhelinverkot, muistinmäärä ja kamera. Näiden ominaisuuksien lisäksi eri käyttöjärjestelmäversiot luovat oman haasteensa [28]. Yhdistelmien määrä kasvaa vieläkin lisää, mikäli mukaan lasketaan lisäksi käyttäjien omat mukautukset, kuten helppokäyttötoiminnot tekstin koon muuttamiseksi, jotka voivat olla mallikohtaisesti erilaiset. Lisäksi täytyy huomioida, että jotkin kielet luetaan vasemmalta oikealle ja osa oikealta vasemmalle. Näiden kaikkien vaihtoehtojen huomioiminen onkin lähes mahdotonta.

Google on kuitenkin tarjonnut erilaisia ratkaisuja, jotka helpottavat sovellusten sovittamista useammille laitteille [29, 27]. Yksi näistä ratkaisuista sisällön ulkoasun määrittämiseksi on mahdollisuus hyödyntää erikokoisia graafisia elementtejä ja niiden mittoja sen mukaan, mitkä laite automaattisesti valitsee sopivimmiksi. Toinen tapa on asettaa sovelluksen asentaminen mahdolliseksi vain laitteisiin, jotka tukevat kaikkia sen vaatimia ominaisuuksia, jolloin sovelluksen suorituksen aikana ei koidu ongelmaa puuttuvasta ominaisuudesta [30]. Tällöin esimerkiksi NFC-piiriä vaativien mobiilimaksusovellusten asennus voidaan estää laitteisiin, joissa ei ole kyseistä NFC-piiriä. Pakollinen NFC-ominaisuus voidaan määrittää *Android Manifest* -määrittelytiedostossa seuraavalla tavalla:

```
<!-- Vaadi käyttöoikeus NFC-piiriin -->
<uses-permission android:name="android.permission.NFC" />

<!-- Aseta NFC pakolliseksi ominaisuudeksi -->
<uses-feature android:name="android.hardware.nfc"
              android:required="true" />
```

Applen iOS -alustalla tilanne on hiukan Androidia helpompi. Apple ei lisensoi iOS-käyttöjärjestelmää muille valmistajille, vaan sitä tarjotaan Applen yksinoikeudella sen omilla laitteilla. Tällöin järjestelmän kehittäjällä on tarkka tieto jokaisesta laitteesta, jolla sitä käytetään, toisin kuin esimerkiksi Androidilla. Käyttöjärjestelmää voidaan täten suunnitella laitteiden mukaan, eikä yleisesti kaikille mahdollisille laitteille. Applen iPhoneja on kirjoitushetkeen mennessä julkaistu 18 eri mallia, Applen iPod Touch -laitteita 6 ja Applen iPadia 15 mallia eli yhteensä 39 erilaista iOS-laitetta kaiken kaikkiaan. [31]

Kuten Androidillakin, myös iOS-järjestelmässä voidaan rajoittaa sovelluksia vai tietyille laitteille tai tietyt ominaisuudet omaaville laitteille [31]. Tällöin käytetään sovelluksen

Info.plist-tiedostoa. Applella on kuitenkin tiukempi politiikka hyväksyttävien sovellusten kehittämiseen ja julkaisemiseen. Esimerkiksi iPhone 6 ja 6 Plus sisältävät NFC-sirun, mutta se on käytössä yksinoikeudella Apple Pay:lle [32] eikä avoimesti kehittäjien käytettävissä [33]. Myöhemmissä malleissa NFC-siru on myös kehittäjien käytettävissä [31].

Mobiilisovelluksesta täytyy lisäksi yleensä kehittää molemmille alustoille omat versionsa mahdollisimman laajan käyttäjäkunnan saamiseksi. Tämä luonnollisesti vaatii molempien alustojen omien vaatimusten täyttämisen erikseen. Olemassa on myös sovelluskehitysympäristöjä, jotka mahdollistavat kehittämisen molemmille alustoille yhtä aikaa, mutta tässä työssä ei keskitytä niihin tämän enempää. Voidaan kuitenkin todeta monipuolisten mobiiliympäristöjen asettavan tiettyjä haasteita mobiilimaksuratkaisujen kehittämiseksi, joita voidaan peilata tarkemmin, kun seuraavassa luvussa esitellään erilaisia lähestymistapoja mobiilimaksuratkaisujen kehittämiseksi.

3. MOBIILIMAKSAMISEN RATKAISUJA

Tässä luvussa perehdytään yleisimpiin Suomessa käytettyihin ratkaisuihin, joilla mobiilimaksamista voidaan toteuttaa. Eri ratkaisut voivat tarjota käyttäjälle samankaltaisia palveluita, mutta niiden toteuttamistapa ja lähtökohta ovat erilaiset. Ratkaisut eivät ota kantaa sovelluksen tekemiseen käytettävään ohjelmointikieleen tai tarjoa valmiita sovelluskomponentteja vaan tarjoavat yleismaailmallisia lähestymistapoja ja malleja. Lisäksi luvussa keskitytään enemmän periaatteisiin ja teknologioihin kuin valmiisiin tuotteisiin tai niiden tarjoajiin. Tällöin kehittäjä voi itse soveltaa saamaansa tietoa tarpeellisella tavalla, riippumatta teknologioista, joilla sovellusta ollaan kehittämässä.

Näitä ratkaisuja ovat token-pohjaiset ratkaisut, joita käsitellään ensimmäisenä alaluvussa 3.1. Niiden jälkeen käsitellään emuloituja fyysisiä maksukortteja ja niillä maksamista alaluvussa 3.2. Kolmantena ja viimeisenä alaluvussa 3.3 käsitellään virtuaalisilla maksukorteilla maksamista, kuten mobiililaittevalmistajien omia maksupalveluita Apple Pay:ta ja Google Pay:ta.

Teknologioita käsitellään järjestyksessä, jossa ensimmäisenä olevassa toteuttajalla on eniten vaikutusmahdollisuuksia toteutukseen ja ominaisuuksiin, jotka vähenevät viimeistä kohti edetessä. Vastaavasti myös kehittämisen työmäärä ja tarvittava tietotaito vähenevät, joka voi puolestaan olla avaintekijänä tätä kaipaavalle toteuttajalle. Eri teknologioissa myös kustannukset koostuvat eri tavoin, joka voi vaikuttaa valittavaan teknologiaan tilanteesta ja käyttötavoista riippuen.

3.1 Token-pohjaiset ratkaisut

Token-pohjaiset mobiilimaksamisen ratkaisut voidaan toteuttaa monilla erilaisilla tavoilla. Token tarkoittaa tässä yhteydessä uniikkia eli yksilöllistä numeroiden ja kirjainten muodostamaa merkkijonoa, jota voidaan käyttää tapahtuman tai istunnon yksilölliseen määrittämiseen ikään kuin allekirjoituksena tai sormenjälkenä [34]. Tällöin järjestelmä ja sovellus voidaan rakentaa puhtaasti näiden tunnisteiden varaan ja suorittaa niillä tarpeellisia operaatioita maksujen käsittelemiseksi. Tämä tarjoaa toteuttajalle paljon räätälöintimahdollisuuksia eri tarpeisiin, sillä siihen on mahdollista liittää mitä vain tarpeellisiksi havaittuja ominaisuuksia, koska koko järjestelmä on toteuttajan suunniteltavana ja toteutettavana.

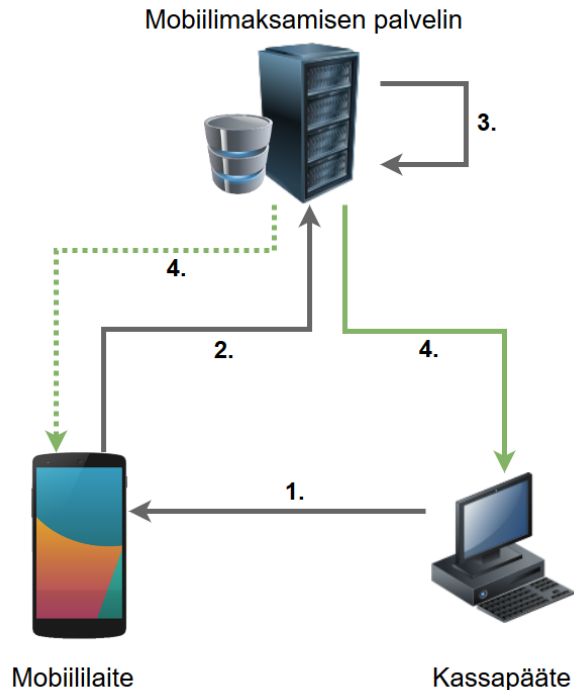
3.1.1 Perusidea

Tällä tavoin kehitetty mobiilimaksaminen perustuu näiden yksilöllisten tokenien siirtoon ja käsittelyyn. Yleensä kaikki käsittely suoritetaan mobiilisovelluksen taustajärjestelmässä erillisellä palvelimella, johon mobiililaitteesta ollaan yhteydessä internet-yhteyden kautta esimerkiksi salattujen HTTPS-kutsujen avulla [35].

Maksun suorittaminen voidaan toteuttaa monilla erilaisilla lähestymistavoilla. Järjestelmän vaatimat viestit ja tiedonsiirto ovat toteuttajan vastuulla, joka tekee kaikkien käytössä olevien tai teoriassa toimivien tapojen luettelemisesta mahdotonta. Tässä kuitenkin esitellään kolme yksinkertaistettua ja rakenteeltaan hiukan erilaista lähestymistapaa tavoitteen saavuttamiseksi. Käytössä voi myös olla useampia palvelimia tai esimerkiksi kaupan omia välityspalvelimia, mutta ne on yksinkertaistuksen nimissä jätetty pois kuvista.

Mobiililaittepainotteinen tapa on, että kassapäätte antaa maksusta kaikki tarvittavat tiedot mobiililaitteelle, joka välittää ne käyttäjän tiedoilla lisättynä palvelimelle, joka suorittaa lopullisen maksun ja ilmoittaa kassapäätteelle maksun onnistumisesta. Maksussa hyödynnetään vastaavia tiedonsiirtoja ja käsittelyvaiheita:

1. *Maksun välitys:* Kassapäätte kokoaa maksun tarpeelliset tiedot ja välittää ne mobiililaitteelle.
2. *Tietojen yhdistely ja välitys:* Mobiililaitte yhdistää maksun tietoihin käyttäjän tietoja ja välittää ne palvelimelle
3. *Prosessointi:* Palvelin tarkistaa maksun tiedot ja käsittelee maksun. Tähän sisältyy tarvittaessa yhteyden ottaminen toiseen palvelimeen tai pankkiin ja varojen siirto, mikäli vastaanottajalla on eri pankki- tai maksupalvelu.
4. *Kuittaus:* Lopuksi palvelin lähettää kuittauksen maksun onnistumisesta tai epäonnistumisesta. Kuittauksen lähettäminen mobiililaitteelle ei ole pakollista, mutta tällöin silläkin voidaan näyttää ilmoitus onnistuneesta tai epäonnistuneesta maksusta.



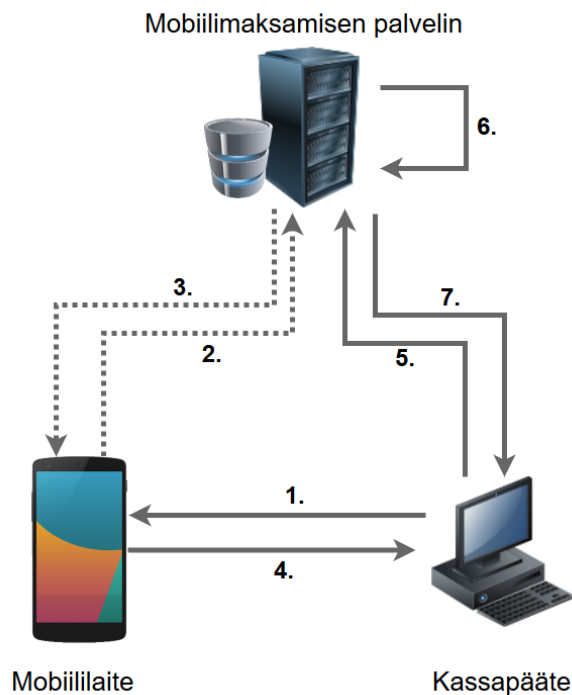
Kuva 3. Yksi tapa mobiilimaksamisessa käytetyistä tiedonsiirroista. Katkoviiva ilmaisee vapaavalintaisen tiedonsiirron. Vihreällä värillä on korostettu yhtäaikainen tiedonsiirto.

Luvun 2 kuvassa 2 kuvattiin tavallisen korttimaksun suoritusta. Yllä olevan kuvan 3 vaiheet 1 ja 2 tapahtuvat vastaavasti kuin korttimaksun vaiheessa 1. *Valinta ja lähetys*. Vastaavasti vaihe 3 sisältää loput vaiheet vaihetta 6. *Kuittaus* lukuun ottamatta, joka tapahtuu kuvan 3 vaiheessa 4 sekä mobiililaitteelle että kassapääteelle. On myös mahdollista lähettää kuittaus jo tietojen tarkistamisen jälkeen, jolloin maksutapahtuma on käyttäjälle nopeampi. Se ei mahdollista myöhemmässä vaiheessa mahdollisesti tapahtuvan virheen huomioimista samalla tavalla. Lisäksi on mahdollista suorittaa enemmän operaatioita, kuin kuvaan on merkattu esimerkiksi paremman tietoturvan takaamiseksi.

Kassapäätelainotteen tapa tarkoittaa järjestelmän kehittämistä siten, että myös kassapääte voi ottaa yhteyttä maksuja käsittelevään palvelimeen. Tällöin mobiililaitte antaa kassapääteelle palvelimelta saamansa tokenin, jonka kassapääte välittää taustapalvelimelle, joka käsittelee maksun. Maksu suoritetaan näiden vaiheiden avulla:

1. *Tietojen kysely:* Kassapääte kysyy mobiililaitteelta tokenin, jolla voidaan tunnistaa käyttäjä.
2. *Tokenin kysyminen:* Mobiililaitte pyytää palvelimelta kertakäyttöisen tokenin. Tämä on vapaavalintaista, sillä on myös mahdollista käyttää aina samaa tokenia. Kertakäyttöiset tokenit kuitenkin mahdollistavat paremman tietoturvan, sillä jälkikäteen tokenin joutuminen väärin käsiin ei tuota ongelmaa.

3. *Tokenin palautus mobiililaitteelle:* Palvelin tunnistaa käyttäjän, luo ja palauttaa kertakäyttöisen tokenin. Tätä vaihetta ei toteuteta, mikäli edellistä vapaavalintaista vaihetta ei toteuteta.
4. *Tokenin palautus kassapääteelle:* Mobiililaitte palauttaa tokenin kassapääteelle.
5. *Maksun välitys palvelimelle:* Kassapääte välittää maksun tiedot palvelimelle.
6. *Prosessointi:* Palvelin tarkistaa maksun tiedot ja käsittelee maksun. Tähän sisältyy tarvittaessa yhteyden ottaminen toiseen palvelimeen tai pankkiin ja varojen siirto, mikäli vastaanottajalla on eri pankki- tai maksupalvelu.
7. *Kuittaus:* Palvelin kuittaa maksun kassapääteelle, joka ilmoittaa maksun onnistumisesta tai epäonnistumisesta.

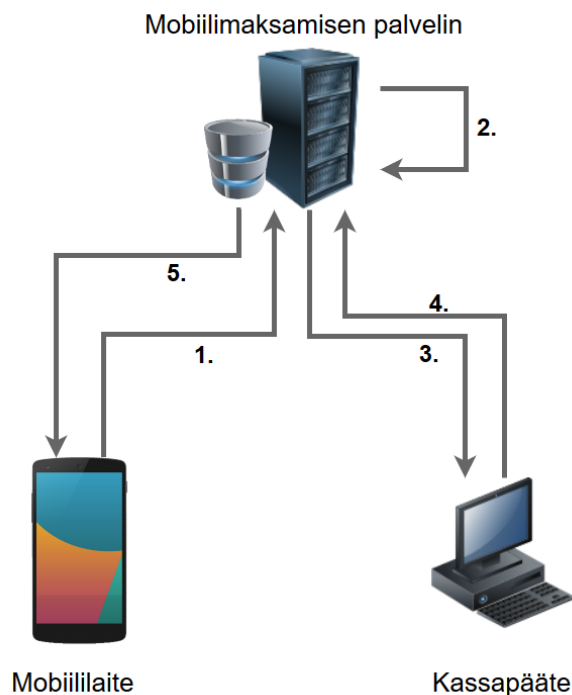


Kuva 4. Toinen tapa mobiilimaksamisessa käytetyistä tiedonsiirroista, jossa kassapääte hoitaa tietojen välittämisen. Katkoviivat ilmaisevat vapaavalintaisen tiedonsiirron.

Kuvasta 4 voidaan huomata, että tässä lähestymistavassa hyödynnetään useampaa vaihetta, kuin ensin esitetystä tavasta. Tämä onkin usein työläämpi tapa, mutta mahdollistaa tokenien kertakäyttöisyyden ja täten mahdollisesti paremman tietoturvan. Tällainen kassapääteen muokkaaminen voi kuitenkin olla työläämpää kuin erillisen mobiilisovelluksen tai taustapalvelun muokkaamisen. Erityisesti, mikäli kassapääte tarvitsee päivitystä tai räätälöintiä tukeakseen tietynlaisia mobiilimaksuja, sillä niihin kohdistuu erillisiä vaatimuksia sekä standardeja [36].

Palvelinpainotteinen tapa ei puolestaan edellytä mobiililaitteen ja kassapääteen välistä kommunikointia ollenkaan, vaan kaikki liikenne tapahtuu palvelimen välityksellä. Tällöin toiminta perustuu oletukseen, jonka mukaan käyttäjä voi valita sovelluksestaan oikean kassan, jonka kanssa suorittaa haluttu operaatio, kuten esimerkiksi mobiilitankkaus. Palvelin käsittelee kutsun ja välittää tiedon oikealle kassapäätteelle.

1. *Maksun välitys:* Mobiililaitte lähettää maksun tiedot palvelimelle.
2. *Prosessointi:* Palvelin tarkistaa maksun tiedot ja käsittelee maksun. Tähän sisältyy tarvittaessa yhteyden ottaminen toiseen palvelimeen tai pankkiin ja varojen siirto, mikäli vastaanottajalla on eri pankki- tai maksupalvelu.
3. *Tieto maksusta välitetään kassapäätteelle:* Palvelin välittää maksun tiedot kassapäätteelle.
4. *Kassapääte kuittaa maksun:* Kassapääte kuittaa palvelimelle saaneensa tiedot maksusta.
5. *Kuittaus:* Palvelin kuittaa maksun mobiililaitteelle, joka ilmoittaa maksun onnistumisesta tai epäonnistumisesta.



Kuva 5. Kolmas tapa mobiilimaksamisessa käytetyistä tiedonsiirroista, jossa mobiililaitte ja kassapääte eivät suoraan vaihda keskenään tietoa.

Tokeneita voidaan siirtää mobiililaitteen ja kassapääteen välillä monin tavoin. Periaatteessa mikä tahansa tapa toimii, jolloin kyse on lähinnä käyttömukavuudesta ja

innovatiivisuudesta. Yksi tapa tokenin siirtämiseen on käyttää hyväkseen monissa mobiililaitteissa olevaa kameraa tokenin skannaamiseen esimerkiksi QR-koodina. QR-koodi on kaksiulotteinen viivakoodi, jonka lukeminen mobiililaitteella on nopeaa ja siihen voidaan tarvittaessa sisällyttää paljonkin tietoa [37]. Token voidaan siirtää myös hyödyntäen kassapääätteen ja mobiililaitteen NFC-sirua. Tällöin maksu muistuttaa ulkoisesti lähimaksua ja HCE-mobiilimaksuratkaisua, sillä mobiililaitetta käytetään kassapääätteen lähellä NFC-yhteyden muodostamiseen ja tiedon siirtämiseen. Tämä toki edellyttää mobiililaitteelta NFC-tukea, jota ei kaikista, etenkin halvemmista laitteista löydy. Toki token voitaisiin siirtää myös kirjoittamalla se mobiililaitteen näppäimistöllä, mutta tämä ei olisi erityisen käyttäjäystävällinen tai nopea tapa, toisin kuin edellä mainitut tavat. Tämä kuitenkin äärimmäisenä esimerkkinä siitä, kuinka monipuolisesti tiedonsiirto voidaan toteuttaa.

3.1.2 Vaatimukset ja haasteet

Tokenien käsittelyyn perustuva mobiilimaksaminen asettaa raskaimmat vaatimuksensa erilaisille taustajärjestelmille ja -palveluille, jotka hoitavat varsinaisen maksun suorittamisen. Tällöin myös suurin työ on näiden järjestelmien kehittämisessä sekä ylläpitämisessä. Toteuttajan vastuulla on myös huolehtia riittävästä tietoturvasta, sekä virhetilanteiden hallitsemisesta ja ratkaisemisesta järjestelmän jokaisessa osa-alueessa [26].

Taustajärjestelmältä vaaditaan lisäksi useita ulkoisia rajapintoja esimerkiksi pankkipalveluiden hyödyntämiseen, mikäli käyttöön halutaan muitakin kuin kaupan omia tilejä ja suoraveloituksia ostajan tililtä jälkikäteen lähetettävän laskun sijaan. Ulkoiset rajapinnat vaativat usein paljon työtä ja saattavat lisätä muitakin vaatimuksia järjestelmälle, jotta niiden käyttö on sallittua. Vuoden 2018 alussa astui voimaan uusi maksupalveludirektiivi, *PSD2*, jonka yhtenä tarkoituksena on helpottaa kolmannen osapuolen palveluntarjoajille pääsyä pankkien palveluihin, rajapintoihin ja tileihin [38, 39, 40]. Tämä todennäköisesti lisää erillisten palveluiden mahdollisuuksia hyödyntää pankin palveluita esimerkiksi mobiilimaksamisen toteuttamisessa, mutta myös aiheuttaa laajemman kilpailun ja mahdollistaa suuremman tarjonnan vastaavista palveluista.

Tokenien ja mobiilimaksujen käsitteleminen vaatii usein myös erillistä tukea käytetyltä kassapääteeltä. Muutosten suuruus riippuu myös siitä, millä lähestymistavalla maksamista on lähdetty rakentamaan ja mikä on kassapäätteen rooli maksun käsittelyssä sekä suorittamisessa.

Lisäksi suurena haasteena on toteuttajan riittävä tietotekninen osaaminen koko järjestelmän suunnittelemiseksi ja kehittämiseksi. Täten monilla mobiilimaksamista suunnittelevilla tahoilla onkin edessään joko osaamisen ostaminen tai järjestelmän tilaaminen ulkopuoliselta taholta. Tämä saattaa merkittävästi nostaa käyttöönottokustannuksia, jotka ovat kehittämistyössä jo muutenkin varsin korkeat tämän kaltaisessa järjestelmässä.

Mobiililaitteelle tämä tapa puolestaan asettaa vain vähän vaatimuksia. Tärkein vaatimus on luonnollisesti tiedonsiirtoon käytetty internet-yhteys, mutta tämä mahdollisuus on löytynyt jo vuosien ajan useimmista jopa kaikkein halvimmista laitteista. Lisäksi useimmista,

jopa kaikkein halvimmista, mobiililaitteista löytyy jonkinlainen kamera, mikäli esimerkiksi QR-koodien lukemista halutaan tukea.

3.1.3 Mahdollisuudet

Vähäiset vaatimukset mobiililaitteiden osalta mahdollistavat laajan tuen useimmille laitteille. Tämä puolestaan tarjoaa mahdollisuuden laajalle kuluttajakunnalle, sillä kuluttajan käytössä oleva mobiililaitte ei rajoita mobiilimaksamisen käyttöönottoa.

Järjestelmän käyttöönottokustannukset voivat olla suuria, mutta vastaavasti käyttökulut pieniä. Mikäli koko järjestelmä on yhden tahon hallinnassa, ei tällöin tarvitse esimerkiksi maksaa käytönmukaista korvausta toisille tahoille, kuten esimerkiksi tavallisen korttimaksamisen kanssa joudutaan toimimaan. Tämä voi auttaa alentamaan suhteellista käyttökustannusta maksutapahtumaa kohti ja suurilla käyttöasteilla tuottaa selkeää säästöä verrattuna korttimaksamiseen tai käteisen käsittelyyn.

Lisäksi täysi järjestelmän hallinta mahdollistaa hyvin monenlaisia räätälöintejä tarpeen mukaan. Näitä ovat esimerkiksi erilaiset edut, joilla voidaan houkutella kuluttajia käyttämään tarjottua mobiilimaksupalvelua. Eduilla voidaan tarkoittaa esimerkiksi ilmaiskuponkeja omiin kohteisiin tai maksutapaetua eli alennusta, mikäli maksetaan mobiilimaksulla. Tällaiset edut voidaan määrittää järjestelmän palvelimelle, joka huolehtii etujen toimittamisesta esimerkiksi maksun yhteydessä. Myös erilliset kanta-asiakas- tai etukortit voidaan liittää suoraan osaksi samaa järjestelmää, jolloin niiden erillinen käyttö ei ole enää tarpeellista, sillä niiden tiedot voidaan haluttaessa yhdistää suoraan palvelimella maksutapahtumaan.

Maksujärjestelmän hallinta mahdollistaa myös kuluttajien käyttötapojen seurannan. Seuranta voidaan liittää sekä mobiilisovellukseen että järjestelmän puolelle. Näiden seurantatietojen avulla on mahdollista analysoida kulutustottumuksia ja siten kehittää omia palveluita kuluttajille sopivammiksi. Laajamittainen seuranta on kuitenkin usein kuluttajien epäsuosiossa, sillä vuonna 2017 Suomessa jopa 60 prosenttia kuluttajista oli huolissaan yrityksien keräämästä ja hallussa olevasta datasta [41].

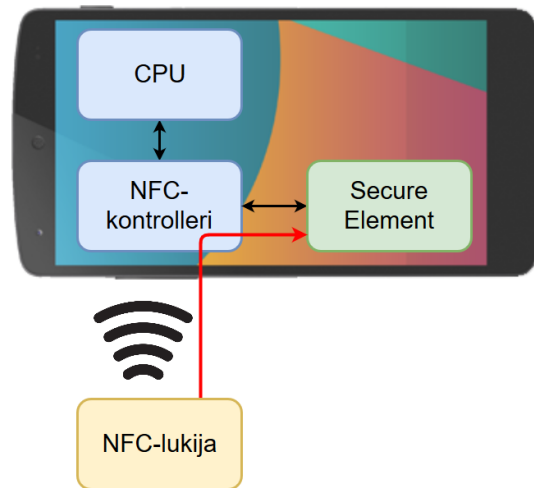
3.2 Fyysinen kortti emuloituna, HCE

Monissa maksukorteissa on nykyään lähimaksuominaisuus. Tämä ominaisuus on vaatinut muutoksia kassojen maksupäätteisiin. Lähimaksuominaisuuksien toteuttaminen NFC-teknologialla mahdollistaa samojen rajapintojen käyttämisen myös mobiililaitteiden NFC-piireillä. Tähän mahdollisuuteen *Host Card Emulation*, tai kuten Google ominaisuutta kutsuu: *Host-based Card Emulation*, tarjoaa oman ratkaisunsa [4]. Mobiililaitteen NFC-piirin avulla on mahdollista vastata maksupäätteen lähimaksamisen kutsuihin samalla tavalla kuin lähimaksua tukeva maksukortti tekisi, jolloin maksuja voidaan suorittaa. Host Card Emulation mahdollistaa siten lähimaksukortin korvaamisen mobiililaitteella, eikä vaadi erillisiä muutoksia olemassa oleviin lähimaksua tukeviin järjestelmiin. Sekä Visa että Mastercard ovat lähteneet vahvasti tukemaan HCE:ta [42, 43] maksuratkaisujen kehittämiseksi.

HCE:ta voidaan hyödyntää myös erilaisten jäsenkorttien ja -etujen toteuttamiseen hyödyntäen samaa NFC-lähimaksurajapintaa, kuin lähiluettavien jäsenkorttien tapauksessa. Tällöin maksupäätteelle ei tietenkään lähetetä maksukortin tietoja vaan etukortin tiedot sopivan muotoisessa viestissä. Mikäli lisäksi halutaan maksaa, se vaatii kuitenkin kaksi erillistä lukukertaa, ensin jäsenkortille ja sitten maksukortille, mikäli näitä kahta ei ole kaupan puolesta yhdistetty toisiinsa.

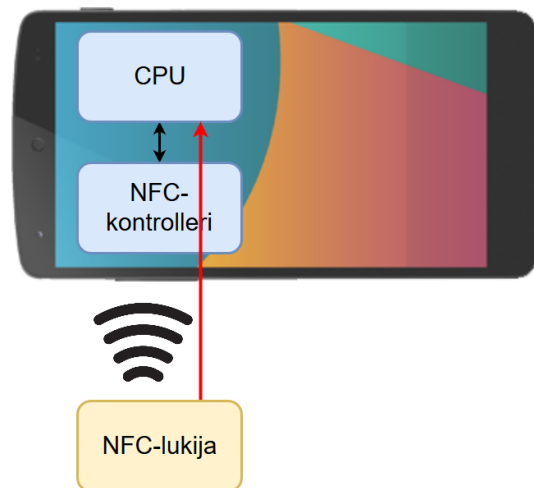
3.2.1 Perustiedot

Host Card Emulationia hyödyntäviä maksuratkaisuja on kahdenlaisia. Maksuun voidaan hyödyntää joistakin puhelimista löytyvää erillistä *Secure Elementiä* tai siihen voidaan käyttää mobiililaitteelta löytyvää sovellusta. Secure Element on mobiililaitteeseen sisällytetty tietoturvallinen säiliö, jonka tehtävänä on tässä tapauksessa tarjota kaikki maksuun tarvittavat maksukortin tiedot, jotka yksinkertaisesti välitetään maksupäätteelle NFC:n avulla ilman maksamiseen tarkoitettua erillistä sovellusta. Mobiililaitteen NFC-piiri osaa tällöin itsenäisesti hakea tiedot ja palauttaa tarpeelliset viestit. Tätä suoraa yhteyttä havainnollistetaan kuvassa 6. Maksusta voidaan haluttaessa kuitenkin ohjata ilmoitus käyttöjärjestelmälle tai sovellukselle. [4]



Kuva 6. Mobiililaitteen NFC-piiri hakee maksukortin tiedot suoraan Secure Elementiltä.

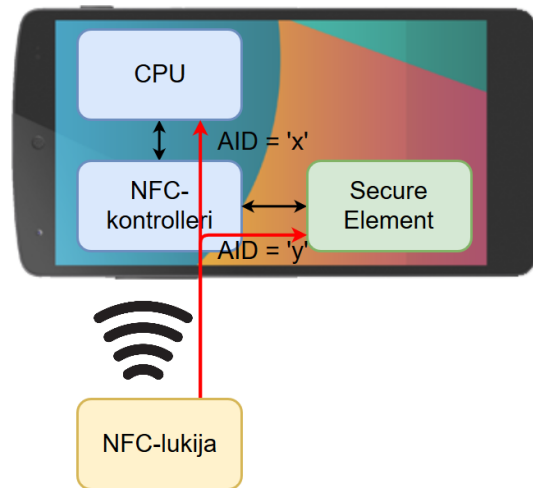
Toisena tapana on hyödyntää mobiilisovellusten mahdollisuuksia dynaamisesti hallita käytössä olevaa tietoa ja täten käytettäviä maksukortteja. Tällöin sovellus huolehtii kuvan 7 mukaisesti oikeanlaisen viestin muodostamisesta ja välittämisestä NFC-piirille ja sitä kautta maksupäätteelle. Tämä mahdollistaa myös sen, että käyttäjä valitsee tapauskohtaisesti, mitä maksukorttia hän haluaa mihinkin maksuun käyttää. Maksukortin valinta voidaan tehdä käynnistämällä jonkin tietyn maksukortin mobiilimaksusovellus. Järjestelmälle voidaan myös asettaa oletusmaksukortti, jota käytetään tilanteessa, jossa käyttäjä ei erikseen valitse mitään korttia. Järjestelmä voidaan myös asettaa kysymään, mitä sovellusta käytetään. [4, 44]



Kuva 7. Mobiililaitteen NFC-piiri hakee maksukortin tiedot prosessorilta, joka saa ne suoritettavalta sovellukselta.

Maksuun käytettävien viestien muoto on kuitenkin sama riippumatta siitä, kumpaa tapaa tietojen luomiseksi tai hakemiseksi käytetään. Lisäksi on mahdollista, että molemmat tavat ovat käytössä samalla mobiililaitteella. Tällöin laitteella täytyy olla ennalta määritelty lista, mitä menetelmää käytetään milläkin *Application ID*:llä eli *AID*:llä, kuten kuvassa 8

esitetään. AID on EMV-ympäristössä käytetty erilaisen maksukorttityypin tunniste, jolla kortit voidaan erotella toisistaan. Listalla määritellään, millä AID:llä tiedot pyydetään Secure Elementiltä ja millä sovelluksilta. [4]



Kuva 8. NFC-ohjaimen ennalta määrätty lista kertoo, mistä tiedot haetaan kyseisellä AID:llä.

Vastaavasti myös käytettävä mobiilimaksusovellus määritetään AID:n avulla. On myös mahdollista, että mobiililaitteelle on asennettu useita samaa AID:tä hyödyntäviä sovelluksia ja maksukortteja. Tällöin hyödynnetään joko oletusmaksusovellusta tai käyttäjän käynnistämää sovellusta. Mikäli sama AID ei ole käytössä useammalla sovelluksella, osaa Android itse valita, mitä sovellusta ja maksukorttia tulee käyttää. [4, 44]

Host Card Emulationia käytettäessä maksutapahtuma alkaa siitä, kun mobiililaitte vastaanottaa maksupäätteen lähettämän *Application Protocol Data Unit (APDU)*:n. APDU on standardin ISO/IEC 7816-4 mukainen tietopaketti, joka voi pitää sisällään maksukortin organisaation ja tyyppin [45]. Tyypillisesti tällä ensimmäisellä viestillä maksupäätte siis pyytää maksukortin tyyppin, johon mobiililaitte vastaa uudella APDU:lla mitä AID:tä käytetään maksamiseen. On myös mahdollista, että maksupäätte tukee vain yhdenlaisia maksukortteja, jolloin jo ensimmäinen viesti sisältää suoraan pyynnön maksaa tietyllä AID:llä varustetulla kortilla. Tämän jälkeen maksupäätte pyytää korttityyppikohtaisia maksuominaisuuksia *Get Processing Options (GPO)*-muotoisessa viestissä, johon vastataan lähettämällä käytössä olevat ominaisuudet. Ominaisuuksiin voi kuulua esimerkiksi, että käytetään Visan MSD-tyyppistä maksutapaa, joka oli ensimmäinen lähimaksun muoto [46, 47]. Ominaisuuksien välittämisen jälkeen pyydetään lopulta itse kortin tietoja maksua varten, johon luonnollisesti vastataan lähettämällä käytetyn kortin tiedot. Tämän jälkeen laitteiden välinen yhteys katkaistaan, sillä maksupäätte on saanut kaikki tarvitsemansa tiedot maksun suorittamista varten. Lisätietoja viesteistä ja niiden välittämisestä myöhemmin alaluvussa 3.2.2. [48, 44, 49, 46]

Mobiililaitteen Host Card Emulationin käyttäminen lähimaksamiseen ratkaisee taval-
listen lähimaksua tukevien maksukorttien kopiointiongelman, sillä NFC-yhteys voidaan
kytkeä pois päältä, kun sille ei ole tarvetta, toisin kuin maksukortista. Tällöin mobiililaitteel-
la sijaitsevan emuloidun maksukortin tiedot eivät ole saatavilla ja kopioitavissa jatkuvasti.
Tämä kuitenkin vaatii käyttäjältä sen, että NFC kytketään aina pois, mikäli sitä ei tarvita, tai
että sovellus pyytää varmistuksen ennen tietojen lähettämistä. Muussa tapauksessa tiedot
voidaan huomaamatta kopioida samalla tavalla kuin maksukortin tapauksessa.

3.2.2 Käyttöönotto

Host Card Emulationin käyttöönotto Android-alustalla aloitetaan toteuttamalla Androi-
din tarjoamaa *HostApuService*-luokkaa laajentava oma luokka, jota käytetään maksujen
käsittelyyn [49]. Java-kielellä laajentaminen toteutetaan avainsanalla *extends*. Täl-
löin laajennetulla luokalla on käytössään kaikki periytetyn *super*-kantaluokan rajapinnat
ja funktiot, joita on mahdollista ylikirjoittaa omilla toteutuksilla käyttäen *@Override*-
avainsanaa. Oma funktio täyttää edelleen saman rajapinnan, mutta sen toiminnallisuutta
voidaan muokata vapaasti. Tässä tapauksessa esimerkiksi lisätään, mitä maksukortteja
halutaan käyttää.

Lisäksi Host Card Emulationin käyttöönottamiseksi on tärkeää määritellä ohjelmakoo-
diin haluttujen standardien mukaiset viestit, jotta niitä voidaan hyödyntää maksupäätteen
viestien tunnistamiseen ja niihin vastaamiseen. Näitä viestejä ovat alla esitetty AID:n
valitsemisen pyytämiseen käytetty *Select AID*, sen vastaukseksi halutun AID:n valinta sekä
valinnan mukainen maksun aloitus. [50] Maksun suorittamiseen käytetty viesti kannattaa
muodostaa dynaamisesti, sillä siihen täytyy sisällyttää käytetyn maksukortin tiedot.

Ohjelma 1. *Select AID APDU -viestin sisältö [50, 46].*

```
private byte [] PPSE_APDU_SELECT = {  
    (byte)0x00, // CLA (komennon luokka)  
    (byte)0xA4, // INS (käsky); 0xA4 = valinta  
    (byte)0x04, // P1 (parametri 1) 0x04 = valitse nimellä  
    (byte)0x00, // P2 (parametri 2)  
    (byte)0x0E, // LC (datan pituus) 14 = "2PAY.SYS.DDF01" pituus  
    // Tämä komento pyytää valitsemaan käytettävän AID:n  
    '2', 'P', 'A', 'Y', '.', 'S', 'Y', 'S', '.', 'D', 'D', 'F', '0', '1',  
    (byte)0x00 // LE (vastauksen maksimipituus, 0 tarkoittaa  
    256)  
};
```

Yllä olevalla viestillä voidaan pyytää minkä tahansa yhteensopivan maksukortin tyyppiä.
Viestin sisältö on hyvin samankaltainen tapauksissa, joissa pyydetään maksua vain tietyllä
korttityypillä. Esimerkiksi *Select AID*-viestin muuttaminen Visa-korttityypin valitsemiseen
tapahtuu korvaamalla valintaan käytetyn viestin "2PAY.SYS.DDF01"sisältö Visan AID:lla
A0000000031010 tavuittain (byte)0xA0, (byte)0x00, (byte)0x00, (byte)0x00, (byte)0x03,

(*byte*)0x10, (*byte*)0x10 ja muuttamalla *LC*-tavuun pituudeksi 0x07 eli lukuarvoltaan 7, mikä on käytettyjen tavujen lukumäärä. Vastaavalla tavalla voidaan muokata valintaviestiä mihin tahansa muuhunkin AID:hen. Seuraavaksi esitellään viesti, jolla voidaan vastata alkuperäiseen *Select AID* -viestiin valitsemalla Visan Credit- tai Debit-kortti.

Ohjelma 2. *Select AID APDU -viestin vastaus, jossa valitaan käytettäväksi Visa Credit- tai Debit-kortti [50, 46]. Viestin sisältö on sisennetty lohkoittain.*

```
private byte [] PPSE_APDU_SELECT_RESP = {
    (byte)0x6F, // FCI (tiedostonhallintamalli)
    (byte)0x23, // LEN (kokonaispituus) 35
    (byte)0x84, // DF (tiedoston nimi)
    (byte)0x0E, // LC (datan pituus) 14 = "2PAY.SYS.DDF01"
        pituus
    // Komento, johon vastataan
    '2','P','A','Y','.','S','Y','S','.','D','D','F','0','1',
    (byte)0xA5, // FCI (valittu tiedostonhallinta)
    (byte)0x11, // LEN (FCI pituus) 17
    (byte)0xBF, // FCI (palvelun valinta)
    (byte)0x0C, // LEN (pituus) 12
        (byte)0x0E, //FCI (nimi)
        (byte)0x61, // DE (tyypin valinta)
        (byte)0x0C, // LEN (valinnan pituus) 12
        (byte)0x4F, // ADF (AID nimi)
        (byte)0x07, // ADF (AID pituus) 7
        // Kerrotaan, että tuetaan AID:tä A0000000031010
        // eli Visa Credit- tai Debit-korttia
        (byte)0xA0, (byte)0x00, (byte)0x00, (byte)0x00,
        (byte)0x03, (byte)0x10, (byte)0x10,
    (byte)0x87, // PRI (tärkeysjärjestyksen valinta)
    (byte)0x01, // LEN (pituus) 1
        (byte)0x01, // PRI (tärkeysjärjestys)
    (byte)0x90, // SW1 (tila) onnistunut = 0x90 0x00
    (byte)0x00 // SW2
};
```

Käsitellään seuraavaksi viestien käsittely ja niihin vastaaminen. Tämä toteutetaan yli-*kirjoittamalla* *HostApuService*-kantaluokan funktio *processCommandApu*. Funktiota kutsutaan sovelluksen ulkopuolelta kantaluokan rajapinnan mukaan. Tällöin funktion paluuarvo välitetään suoraan NFC-piirille, joka toimittaa sen eteenpäin pyynnön lähittäneelle laitteelle, kuten maksupäätteelle. Mikäli vastausviestiä ei voida heti välittää, voidaan palauttaa tyhjä arvo *null* ja vasta sitten oikea vastausviesti *sendResponseApu*-funktiolla, kun se on saatu käsiteltyä. [49]

Ohjelma 3. Oma maksupalveluluokka *MyPaymentService*, joka laajentaa Androidin *HostApuService*-luokkaa ja ylikirjoittaa *processCommandApu*-funktion [49].

```
public class MyPaymentService extends HostApuService {
    ...
    // Käytännössä kannattaisi muodostaa dynaamisesti
    private byte[] cardData = ...;
    private byte[] UNKNOWN_RESPONSE = {(byte)0x6F, (byte)0x00};

    // receivedApu parametrissa on vastaanotettu APDU.
    // bundle parametria käytetään tarvittaessa lisätietoihin.
    // Paluuarvoksi välitetään vastaus.
    @Override
    public byte[] processCommandApu(byte[] receivedApu, Bundle
        bundle) {
        byte[] responseApu = null;

        // Vertaillaan, minkä tyyppinen pyyntö maksupäätteeltä
        // on tullut ja vastataan halutunlaisella viestillä
        // lähettämällä se funktion paluuarvona
        if (Arrays.equals(PPSE_APU_SELECT, receivedApu)) {
            responseApu = PPSE_APU_SELECT_RESP;
        } else if (Arrays.equals(PPSE_VISA_SELECT, receivedApu)) {
            responseApu = VISA_SELECT_RESPONSE;
        } else if (isGpoCommand(receivedApu)) {
            responseApu = GPO_COMMAND_RESPONSE;
        } else if (Arrays.equals(READ_CARD_COMMAND, receivedApu)) {
            responseApu = cardData;
        } else {
            responseApu = UNKNOWN_RESPONSE;
        }
        return responseApu;
    }
    ...
}
```

Lopuksi sovelluksen toiminnan kannalta on tärkeää päivittää sovelluksen määrittelytiedosto Android Manifest ajan tasalle. Normaalien näkymien ja sovelluksen oikeuksien lisäksi Manifestiin tarvitsee nyt lisätä erillinen maksupalvelun määrittely [49]. Lisäksi selkeyden vuoksi tuetut AID:t voidaan listata erilliseen XML-tiedostoon, johon Manifestista voidaan viitata käyttämällä hyödyksi Androidin resurssienhallintaa ja sen @-syntaksia *android:resource="@xml/aid_list"*, joka hakee XML-tyyppisistä resursseista kyseisellä nimellä varustettua tiedostoa. Vastaavalla syntaksilla voidaan hakea esimerkiksi merkkijonoja tai lukuarvoja. Tällöin Manifestiin lisättävä määrittely näyttää seuraavalta:

Ohjelma 4. Maksupalvelun lisääminen Android Manifestiin. [49]

```

<!-- Määritellään omasta palveluluokasta yleinen palvelu
      exported-avainsanalla ja sidotaan siihen NFC:n käyttöoikeus
-->
<service android:name=".MyPaymentService" android:exported="
      true" android:permission="android.permission.
      BIND_NFC_SERVICE">
<!-- Määritellään, miten palvelu voidaan käynnistää -->
      <intent-filter>
            <action android:name="android.nfc.cardemulation.action.
            HOST_APDU_SERVICE"/>
      </intent-filter>
<!-- Lisätään erillisestä tiedostosta sallitut AID:t -->
      <meta-data android:name="android.nfc.cardemulation.
      host_apdu_service" android:resource="@xml/aid_list"/>
</service>

```

Ja tältä esimerkiksi määritelty tuettujen Application ID:iden määrittelytiedosto aid_list.xml näyttää:

Ohjelma 5. Tuettujen Application ID:iden lista. [49]

```

<!-- Alustetaan XML-tyyppi -->
<host-apdu-service xmlns:android="http://schemas.android.com/
      apk/res/android"
<!-- Haluttaessa tähän voidaan liittää kuvaus resursseista -->
      android:description="@string/service_description"
<!-- Vaatiiko käyttö lukituksen poistoa vai ei -->
      android:requireDeviceUnlock="false">
<!-- Määritellään uusi AID-ryhmä ja sen kuvaus -->
      <aid-group android:description="@string/aid_description"
<!-- Valitaan kategoria: "other" tarkoittaa pieniä toimijoita
      ja "payment" yleiskäyttöisiä lähes kaikkialla toimivia
      sovelluksia -->
      android:category="other">
<!-- Listataan sallitut AID:t -->
      <aid-filter android:name="A1111111111111111"/>
      <aid-filter android:name="A2222222222222222"/>
      </aid-group>
</host-apdu-service>

```

Näiden ylläesitettyjen ohjelmakoodien avulla on mahdollista toteuttaa yksinkertainen maksupalvelusovelluksen runko Androidille. Muille alustoille toteuttaminen vaatii luonnollisesti hiukan erilaisen lähestymistavan, mutta yllä esitettyjen APDU-viestien sisältö on tietenkin standardin mukaisesti sama. On myös tärkeää huomata, että yllä olevat esi-

merkit eivät välttämättä takaa korkeaa tietoturvaa, vaan tarjoavat pohjan, jonka avulla voi lähteä liikkeelle ja ymmärtää Host Card Emulationin toiminnan perusajatuksen. Lisäksi erilaisten maksukorttien tiedot täytyy selvittää erikseen yleensä yhteistyössä pankkien ja maksukorttien liikkeellelaskijoiden kanssa.

3.2.3 Vaatimuksia ja haasteita

Host Card Emulationin käyttö ei kuitenkaan vapauta perinteisten maksukorttijärjestelmien käytöstä, sillä toiminta perustuu olemassa olevien maksukorttien emuloimiseen. Lisäksi tarvitaan jokin keino, jolla järjestelmässä olevien maksukorttien tiedot saadaan turvallisesti rekisteröityä mobiilimaksusovellukseen. Periaatteessa olisi mahdollista puhtaasti kopioida kortti käyttäen NFC-piiriä, mutta tämä mahdollistaisi myös muiden kuin käyttäjän omien maksukorttien liian helpon kopioimisen. Lisäksi suora kopioiminen saattaa rikkoa maksukorttien käyttöehtoja valmistajasta riippuen. Näistä syistä kopioiminen on yleensä poissa laskuista tämän ominaisuuden toteuttamiseksi.

HCE vaatii myös maksujärjestelmän maksupäätteiltä lähimaksuominaisuuksien tukea. Tämä saattaa vaatia lisäkehitystä ja päivityksiä maksupäätteisiin, mikäli ne eivät ennestään tue kyseisen korttityypin lähimaksua. Lisäkehitys voi osoittautua kalliiksi, sillä se joudutaan usein tilaamaan maksupäätteen tarjoajalta erikseen, minkä lisäksi päivittäminen voi olla työlästä.

Lisäksi yhden haasteen tuo myös mobiililaitteen mahdollinen varkaus. Tällöin erityisen ongelmalliseksi muodostuvat mobiilimaksusovellukset, jotka sallivat maksamisen ilman lukituksen poistamista. Tällaiset sovellukset mahdollistavat varkaalle vapaan käytön tallennetuille maksukorteille. Varkautapauksessa maksukortin käyttäminen voidaan kuitenkin estää sulkemalla kyseinen kortti. Tämä luonnollisesti estää sekä alkuperäisen kortin että emuloidun kortin käyttämisen. Toinen keino välttää luvaton käyttö on vaatia käyttäjän tunnistautumista esimerkiksi sormenjäljen avulla.

Erilaiset laitteet

HCE:n hyödyntäminen vaatii luonnollisesti mobiililaitteelta NFC-tukea, jonka lisäksi sovelluksen täytyy pyytää järjestelmältä piirin käyttöön lupa luvussa 2.2.2 esitetyllä tavalla. Tämä rajoittaa potentiaalista käyttäjäkuntaa, sillä jokaisesta mobiililaitteista ei löydy kyseistä NFC-tukea. Lisäksi kaikki iPhone-puhelimet ovat rajautuneet ominaisuuden käytön ulkopuolelle Applen rajoitettua puhelinten NFC-piirin käyttöä. Tämä on merkittävä heikkous, sillä sen takia ei ole mahdollista tarjota vastaavaa maksuratkaisua molemmille suurille alustoille.

HCE:n tukeminen lisättiin Androidiin versiossa 4.4 eli API level 19:n mukana vuonna 2013 [4]. Tämä rajaa tätä vanhemmat mobiililaitteet pois ominaisuuden piiristä, vaikka niistä NFC-tuki löytyisikin. Nykyään tällaiset Android-versiot ovat kuitenkin pienessä, 5,7

prosentin marginaalissa [29]. Lisäksi vanhenevilla versioilla on luonnollisesti entisestään vähenevä rooli uusien versioiden tullessa markkinoille.

Oman haasteensa tuo myös joidenkin Android-käyttäjien itse vaihtama mobiililaitteen käyttöjärjestelmä tai pääkäyttäjän oikeuksien avaaminen eli ns. *roottaus*. Nämä muutokset saattavat poistaa mobiililaittevalmistajan asettamat suojaukset tai tarjota mahdolliselle hyökkääjälle enemmän vapauksia järjestelmän sisällä. Tämä saattaa asettaa myös tallessa olevat maksukortin tiedot vaaraan. Yleisesti monien pankki- ja maksusovelluksien käyttäminen tällaisilla laitteilla on erikseen estetty juuri tästä syystä.

Fyysisten maksukorttien emuloiminen on mahdollista Androidin lisäksi BlackBerry OS 7 ja sitä uudemmilla versioilla [51] sekä Windows 10 -käyttöjärjestelmällä [52]. Molemmat ovat kuitenkin pienessä marginaalissa mobiililaittepuolella verrattuna Androidiin ja iOS:ään. Windows 10 -tuki voi kuitenkin mahdollistaa myös kannettavien tietokoneiden ja erilaisten hybridilaitteiden käytön maksamiseen, joka voi olla merkittävä tekijä erityisesti yritysasiakkaiden tapauksessa.

3.3 Virtuaalinen maksukortti

Virtuaaliseen korttiin perustuvat maksuratkaisut ovat usein pohjimmiltaan kahden edellä mainitun ratkaisun välimalleja. Palveluissa taustalla on usein edelleen fyysinen maksukortti, mutta jokainen asiakkaan ja kauppiaan välinen maksu käsitellään yksilöllisten tokenien avulla [53, 32]. Tällainen järjestelmä on toki mahdollista kehittää myös itse, kuten monet toimijat ovat tehneetkin, mutta toteutuksen ollessa verrattain lähellä edellä esitettyjä ratkaisuja, paneudutaan tässä luvussa ulkopuolisten tahojen tarjoamien ns. PayPalveluiden käyttöönottamiseen. Lisäksi käsitellään tällaisiin ratkaisuihin varsinaisesta palveluntarjoajasta riippumattomia yhteneviä piirteitä ja ominaisuuksia.

Mobiilimaksamisen yleistyminen on kuitenkin ollut Suomessa hitaampaa kuin muissa Pohjoismaissa, mikä aiheuttaa painetta valmiimpien ulkomaisten ratkaisujen käyttöönottomiseksi myös Suomessa [54]. Osa näistä ratkaisuista on ollut pelkästään kyseisen pankin omassa käytössä ja muutamia harvoja, kuten tanskalaisen Danske Bankin MobilePay:ta, on ollut mahdollista käyttää myös muiden pankkien maksukorteilla. MobilePay onkin Suomessa käytetyin mobiilimaksupalvelu. Vuoden 2018 uusi maksupalveludirektiivi, PSD2, todennäköisesti mahdollistaa entistä enemmän rajapintojen hyödyntämistä pankkien välillä mahdollistaen helpommin useampaa eri pankkia tukevia sovelluksia.

Monet suuret mobiilijärjestelmäkehittäjät, kuten Google ja Apple, ovat kuitenkin lähteneet mukaan mobiilimaksamisliiketoimintaan [53, 32] tarjoamalla avoimia ratkaisuja, joihin pankit ja muut maksamisratkaisujen tarjoajat voivat hakea mukaan. Ne pyrkivät tarjoamaan kuluttajille mahdollisimman helpon tavan hyödyntää mobiilimaksamista omalla mobiililaitteellaan ja käyttävät tätä yhtenä markkinointikeinona oman alustansa puolesta. Tähän helppouteen liittyy kuitenkin ongelma maksukorttipalveluita tarjoavia yrityksiä ajatellen, sillä palvelun pyörittäminen on vain ja ainoastaan valmistajan itsensä käsissä, eikä palvelu siten ole muokattavissa omiin tarpeisiin sopivaksi.

3.3.1 Perustiedot

Yksi suurimmista eduista ulkopuoliseen palveluun turvautuessa on, ettei uusille järjestelmille tai olemassa olevien päivittämiselle ole välttämätöntä tarvetta. Tämä tekee käyttöönoton kevyeksi ja nopeaksi, mikäli sopiva palveluntarjoaja löytyy yhteistyökumppaniksi. Luonnollisesti käyttöönotto täytyy kuitenkin neuvotella palveluntarjoajan kanssa ja sopia palvelun hyödyntämisestä sekä sopimuksen ehdoista. On kuitenkin hyvä muistaa, että vaikka käyttöönottoon ei sisältyisikään suuria kustannuksia, on palvelussa todennäköisesti muita maksuja esimerkiksi käyttömäärän mukaan.

Jo pelkästään riippuvuuden kasvamisen takia tämä ratkaisu ei välttämättä sovi kaikille tahoille. Oman liiketoiminnan uskominen ulkopuolisen palveluntarjoajan käsiin vähentää omia vaikutusmahdollisuuksia sekä saattaa lisätä ennalta-arvaamattomia tilanteita, joihin ei välttämättä ole edes mahdollisuutta itse vaikuttaa. Täten onkin olennaista sopia etukäteen esimerkiksi, miten yllättävissä virhetilanteissa tai käyttökatkoissa toimitaan.

Lisäksi ulkopuolisen palvelun hyödyntäminen mahdollistaa tälle palveluntarjoajalle keinoja seurata kuluttajia sekä näiden toimia ja hyödyntää tätä dataa haluamallaan tavalla oman toimintansa kehittämiseksi. Tämä saattaa avata myös oman businesslogiikan saloja ulkopuolisille tahoille, jotka saattavat pahimmassa tapauksessa olla suoria kilpailijoita samalla alalla. Samalla myös omat mahdollisuudet tämän datan hyödyntämiseksi poistuvat, ellei siitä ole erikseen sovittu palveluntarjoajan kanssa.

Hyvinä puolina voidaan kuitenkin vielä todeta käyttäjien helppo hankkiminen, sillä esimerkiksi Apple Pay -sovellus löytyy valmiina kaikista uusista iPhone-puhelimista ja iPad-taulutietokoneista [32], jolloin käyttäjän ei tarvitse erikseen asentaa uutta sovellusta mobiililaitteelleen. Sama pätee myös palveluihin, jotka jo valmiiksi tukevat useampia erilaisia maksukortteja, sillä tällöin käyttäjällä saattaa olla kyseinen mobiilimaksusovellus jo valmiiksi asennettuna toisen palvelun käyttämiseksi. Näissä tilanteissa pelkkä maksukortin rekisteröiminen palveluun riittää, mikä saattaa laskea kuluttajien kynnystä ottaa palvelu käyttöön.

3.3.2 Käyttöönotto

Käyttöönotosta sovitaan yksilökohtaisella sopimuksella palveluntarjoajan kanssa. Nämä sopimukset ovat usein salaisia, eikä niistä ole saatavilla juuri mitään julkista tietoa. Palveluntarjoajiin voi kuitenkin joka tapauksessa ottaa yhteyttä sekä tiedustella ja neuvotella sopimuksen ehdoista ennen sen hyväksymistä. Palvelun ehdoista on äärimmäisen tärkeää neuvotella jo etukäteen, jotta sopimuksen molemmat osapuolet ovat selvillä siitä, mitä on sovittu ja miten erilaisissa tilanteissa toimitaan, sekä luonnollisesti myös muodostuvista kustannuksista.

Käyttöönotto saattaa vaatia lisäksi päivityksiä omiin järjestelmiin tai kassapäätteisiin, jotta ne tukevat tätä ulkopuolisen tahon tarjoamaan palvelua [32]. Tämä voi tarkoittaa esimerkiksi maksupäätteiden NFC-tukea lähimaksujen suorittamiseen, mikäli sitä ei ennestään ole käytettävissä, tai uuden varmennuspalvelimen osoitteen lisäämistä kassapäätteisiin, jotta uudentyypiset maksut osataan varmentaa ja suorittaa oikein. Monet palveluntarjoajat kuitenkin tarjoavat tähän mahdollisimman helppoja ratkaisuja laajentaakseen palveluun liittyneiden, kyseistä maksutapaa tukevien kauppojen ja liikkeiden verkostoa, jotta mahdollisimman suuren tuen ansiosta palvelusta tulisi kuluttajille entistäkin houkuttelevampi vaihtoehto.

3.3.3 Vaatimukset

Ulkopuolisen tahon kehittämä ja tarjoama palvelu toimii luonnollisesti vain niissä kohteissa ja käyttötapauksissa, joissa palveluntarjoaja on tarkoittanut sen toimivan. Tämä saattaa rajoittaa mahdollisesti lukuisia kauppiaita, maksupääteteknologioita tai mobiililaitteita kokonaan käytön ulkopuolelle. Esimerkiksi Googlen, Applen tai jonkin muun mobiililaittevalmistajan ratkaisun käyttöönotto rajaa muut mobiililaitteet tai käyttöjärjestelmät

ratkaisun ulkopuolelle [53, 32]. Tällöin voi olla välttämätöntä tehdä sopimus useamman eri palveluntarjoajan kanssa, jotta mahdollisimman monille käyttäjille voidaan tarjota vastaavaa palvelua mobiililaitteesta riippumatta. Tämä voi koitua ongelmaksi, mikäli jokin palveluntarjoaja vaatii yksinoikeutta tarjota palvelua ja estää täten solmimasta vastaavaa sopimusta toisen palveluntarjoajan kanssa.

Myös palvelun kehittäminen ja sovittaminen uusiin käyttökohteisiin on viime kädessä täysin palveluntarjoajan omissa käsissä. Uusista ominaisuuksista voi toki aina koettaa neuvotella, mutta niiden toteutumisesta tai itselle koituvista kustannuksista on mahdotonta tietää ennalta, mikäli palveluntarjoaja suostuu ehdotettuihin muutoksiin. Tämä saattaa asettaa erityisiä paineita valita mahdollisimman soveltuva palveluntarjoaja sekä perehtyä kaikkiin mahdollisuuksiin ennen lopullisen päätöksen tekoa.

4. VERTAILU

Seuraavaksi vertaillaan edellä esiteltyjä teknologiaratkaisuja keskenään. Vertailun keskeisinä kriteereinä toimivat kehitys- ja käyttökustannukset eri tilanteissa sekä räätälöitävyys eli mahdollisuus valita tarpeeseen parhaiten soveltuvat ominaisuudet. Yhdessä nämä tekijät muodostavat pohjan, jonka avulla voidaan lähteä arvioimaan eri ratkaisujen sopivuutta.

4.1 Kehityskustannukset

Todellisten kehityskustannusten arvioiminen on vaikeaa, sillä ne riippuvat hyvin monista asioista. Olennaisena osana kustannuksiin on vaikuttamassa haluttujen ominaisuuksien määrä sekä toimintaympäristö, jossa järjestelmän halutaan toimivan. Tulevissa esimerkeissä on käytetty karkeita arvioita minimitoteutuksen kustannuksista osoittamaan suhteellista suuruusluokkaa verrattuna muihin vaihtoehtoihin.

Seuraavissa esimerkkikustannusarvioissa on hyödynnetty mahdollisia euromääräisiä kustannuksia. Euroina esitetyt kustannukset mahdollistavat helposti suoran vertailun eri ratkaisujen välillä sekä mahdollistavat käyttökustannusten lisäämisen samaan vertailuun. Ongelmana tässä kuitenkin on, että todellinen summa riippuu paljolti siitä, kuka todellisen kehityksen toteuttaa ja paljonko siitä laskutetaan. Toinen vaihtoehto olisi arvioida kustannuksia työhön mahdollisesti kuluvan ajan perusteella. Tässäkin on kuitenkin ongelmansa, sillä se riippuu jälleen paljon siitä, kuinka nopeita kehittäjät todellisuudessa ovat.

Token-pohjaisilla järjestelmillä kehityskustannukset ovat vertailluista ehdottomasti suurimmat, sillä siihen kuuluu mobiilisovellusten lisäksi myös taustajärjestelmä. Vaikka tässä työssä taustajärjestelmää ei olekaan juuri käsitelty, on siitä koituvia kustannuksia kuitenkin syytä huomioida koko ratkaisua ajatellessa. Merkittävässä roolissa on myös, kuinka montaa mobiilikäyttöjärjestelmää halutaan tukea, sillä jokaiselle alustalle täytyy kehittää oma sovelluksensa. Käytetään edellä suuntaa antavaa kustannusarviota järjestelmästä, jossa on taustajärjestelmän lisäksi kehitettävä molemmille suurille mobiilikäyttöjärjestelmille omat versionsa. Tällöin kehityskustannukset voivat olla noin 100 000 euroa. Toki halvemmallakin saattaa olla mahdollista toteuttaa vastaava järjestelmä, mutta todelliset kustannukset voivat olla myös paljon tätäkin suuremmatkin.

Host Card Emulation -pohjainen ratkaisu puolestaan on kevyempi kehittää, sillä siihen ei tarvita erillistä taustajärjestelmää. Lisäksi kyseistä ratkaisua ei ole mahdollista kehittää Applen iOS-käyttöjärjestelmälle, joten kehityskustannukset koostuvat yhden mobiilisovelluksen kehittämisestä. Kustannukset riippuvat paljolti siitä, mitä kaikkia

ominaisuuksia sovellukseen halutaan. Voidaan kuitenkin arvioida kehityskustannuksiksi noin 30 000 euroa.

Ulkopuolisten Pay-palveluiden tapauksessa varsinaisia kehityskustannuksia ei ole ollenkaan, sillä palveluntarjoaja on vastuussa järjestelmän kehittämisestä ja ylläpidosta. Palvelusta riippuen on kuitenkin mahdollista, että käyttöönottoon liittyy jokin avausmaksu tai muu kustannus, joka tietenkin kannattaa huomioida mukaan, mikäli tällaisesta on tietoa palveluntarjoajaa valittaessa.

4.2 Käyttökustannukset

Useiden maksutapojen kustannukset riippuvat suoritettujen maksujen suuruudesta. Keskimääräinen korttimaksun suuruus Suomessa oli 29,50 euroa vuonna 2015 [55], joten voimme hyödyntää tätä keskimääräistä arvoa käyttökustannusten laskemiseksi, vaikka kustannuksiin voikin vaikuttaa myös muita tekijöitä. Arviot voivat kuitenkin helpottaa todellisten kustannusten vertailua.

Host Card Emulationia hyödyntävät mobiilimaksuratkaisut noudattavat samoja kauppiaalle koituvia kustannuksia kuin alkuperäisellä maksukortilla maksettaessa. Visa- ja Mastercard-tyyppisillä Debit-korteilla maksettaessa kustannukset ovat 0,31% maksun suuruudesta, kuitenkin vähintään neljä senttiä ja enintään 75 senttiä maksutapahtumaa kohden [56]. Keskimääräisen maksun kustannus on täten 9,1 senttiä. Credit-kortilla kustannus puolestaan on kortin tarjoajasta riippuen keskimäärin 0,9% [56]. Tällöin keskiostoskustannus on 26,6 senttiä. Osa kauppiaista kuitenkin veloittavat nämä kulut suoraan asiakkaalta, aivan kuten tavallistenkin korttimaksujen tapauksessa.

Token-pohjaisissa järjestelmissä maksusta ei itsessään koidu varsinaisia kustannuksia, sillä kaikki toiminnot käsitellään oman järjestelmän piirissä. Ylläpidosta ja järjestelmän resurssien, kuten laskentatehon tai verkkoyhteyden, käytöstä kuitenkin koituu yleensä hiukan kustannuksia. Yksittäisen tapahtuman käsittelyn kustannukset ovat kuitenkin varsin pienet. Pyöristetään ne tässä esimerkissä yhteen senttiin, jotta kulut kuitenkin pysyvät laskuissa mukana, vaikka todellisuudessa kustannukset voivat olla tätäkin matalampia.

Ulkopuolisten Pay-palveluiden hyödyntämisen kustannuksia puolestaan on vaikea arvioida. Luotettavaa tietoa eri tahojen välisistä sopimuksista etenkin Euroopassa ei ole juurikaan julkisesti saatavilla. Apple Pay:n kustannusten pankeille arvioidaan kuitenkin olevan 0,15% Credit-kortilta ja noin 0,42 senttiä Debit-kortilta [57, 58]. Lisäksi Apple on linjannut, ettei maksusta saa koitua kustannuksia asiakkaalle eikä kauppiaille, vaan tällöin ne jäävät käytetyn maksukortin liikkeellelaskijan maksettavaksi [32]. Google Pay:n käytöstä puolestaan ei ainakaan toistaiseksi peritä vastaavia maksuja johtuen Googlen, Visan ja Mastercardin välisestä sopimuksesta [58], joka voi tehdä alustasta pankkien kannalta mielenkiintoisemman valinnan. Google Pay ei kuitenkaan toistaiseksi ole käytössä Suomessa.

Suomen suosituimpaan mobiilimaksupalveluun, MobilePayhin, ei myöskään kuulu käytöstä aiheutuvia kustannuksia, mutta maksujen vastaanottamisesta peritään kauppiaalta

maksu [59]. Mikäli tarkoituksena on tarjota mobiilimaksupalvelu ilman tarvetta omissa liikkeissä tapahtuvalle maksamiselle, ei näitä perittäviä maksuja tarvitse huomioida yhtä paljon. Päinvastaisessa tilanteessa nämäkin kustannukset on kuitenkin syytä huomioida. Maksun vastaanottaminen MobilePayn pienyrittäjille suunnatun mobiilissa toimivan MyShop-palvelun kautta maksaa käyttömäärästä riippuvaisen summan, kuitenkin minimissään 6 senttiä tapahtumalta [60]. Alle 2 000 tapahtumaa vuodessa maksavat tapahtumaa kohden 0,75%, 2 000-9 999 tapahtumaa puolestaan maksavat 0,5% ja korkein taso eli yli 10 000 tapahtumaa maksavat enää 0,35% [60]. Lisäksi MobilePay tarjoaa kassapäätteeseen integroitavaa palvelua, mutta sen kustannuksista ei ole julkista tietoa.

Vaikka esitettyjen vaihtoehtojen vertailu ei annakaan täysin luotettavaa kuvaa kaikkien Pay-palveluiden kustannuksista, voidaan muiden palveluiden kustannuksia kuitenkin arvioida näiden tietojen perusteella. Eri vaihtoehtojen on toisistaan merkittävästi vaihteleva kustannusrakenne. Tämä vaikeuttaa koko ratkaisun käyttökustannusten vertailua token-pohjaiseen järjestelmään ja Host Card Emulationiin, sillä vertailukohdaksi ei ole asettaa yksioikoista arvoa. Selkeyden vuoksi voimme kuitenkin arvioida kustannusten olevan noin käytössä olevien esiteltyjen vaihtoehtojen keskiarvo.

Debit-kortille kustannusportaat olisivat tällöin 13,2 senttiä ostotapahtumalta, 9,5 senttiä ja 7,2 senttiä. Vastaavasti kustannusportaat Credit-kortille ovat 0,45% eli 13,3 senttiä, 0,33% eli 9,7 senttiä ja 0,25% eli 7,4 senttiä. Laskennassa käytetyllä keskiverto-ostoksen summalla sekä Credit- että Debit-korteilla kustannukset ovat hyvin lähellä toisiaan. Ero kuitenkin suurenee keskivertoa suuremmilla ostoksilla, sillä Apple Pay -palvelussa Debit-kortin ostoilla on kiinteä hinta, kun taas Credit-kortin ostoilla summasta riippuvainen 0,15%. Todelliset kustannukset selviävät kuitenkin vasta neuvottelemalla palveluntarjoajan kanssa sopimuksesta.

Taulukko 1. Arvioidut kokonaiskustannukset erilaisten käyttötärpeiden mukaan Debit-korteilla. Summat ovat euroina.

	Token	HCE	Ulkopuolinen
Kehityskustannukset	100 000	30 000	0 - X
Yksittäinen tapahtuma	0,01	0,091	0,132, 0,095 ja 0,072
1 000 tapahtumaa	10	91	132
5 000 tapahtumaa	50	455	475
10 000 tapahtumaa	100	910	720
100 000 tapahtumaa	1 000	9 100	7 200
500 000 tapahtumaa	5 000	45 500	36 000

Token-pohjaisen järjestelmän voidaan huomata olevan ehdottomasti halvin käyttökustannusten mukaan, mutta se on 500 000:lla ostotapahtumalla edelleen kokonaisuutena kallein, kun mukaan lasketaan myös kehityskustannukset. HCE ja ulkopuoliset Pay-palvelut siirtyvät kuitenkin suurilla ostotapahtumamäärillä kalliimmiksi ratkaisuuksi. Näillä suurilla

ostomäärillä Host Card Emulation on kiistatta kallein ratkaisu, vaikka ero Pay-palveluihin ei olekaan valtavan suuri.

Pienillä ostomäärillä ulkopuolisen Pay-palvelun käyttäminen sen sijaan on ehdottomasti halvin ratkaisu. Kehityskustannuksiin ei automaattisesti kuulu suurta summaa, jonka lisäksi käyttökustannukset ovat vain melko vähän HCE:tä korkeammat. Pay-palveluiden tapauksessa kannattaa kuitenkin muistaa, että todelliset käyttökustannukset voivat erota merkittävästi arvioiduista kustannuksista.

Host Card Emulationin kokonaiskustannukset ovat samalla tasolla token-pohjaisen järjestelmän kanssa reilun 864 000 ostotapahtuman kohdalla. Tämän jälkeen token-pohjainen järjestelmä on kokonaisuutena halvempi ratkaisu kuin HCE. On kuitenkin syytä muistaa, että puhutaan euromääräisesti todella suuresta kokonaismyynnistä, kun tuo ostotapahtumien määrä toteutuu. Tapahtumien kustannukset on laskettu keskimääräisellä 29,50 euron ostoksella, jolloin taulukon 1 000 tapahtumaa on arvoltaan 29 500 euroa ja 500 000 tapahtumaa peräti 14,75 miljoonaa euroa. Tällöin ratkaisujen kustannukset ovat tasoissa, kun kokonaismyynti on noin 25,5 miljoonaa euroa. Seuraavaksi vertaillaan vastaavia järjestelmiä Credit-korttien kustannuksilla.

Taulukko 2. Arvioidut kokonaiskustannukset erilaisten käyttötärpeiden mukaan Credit-korteilla. Summat ovat euroina.

	Token	HCE	Ulkopuolinen
Kehityskustannukset	100 000	30 000	0 - X
Yksittäinen tapahtuma	0,01	0,266	0,133, 0,097 ja 0,074
1 000 tapahtumaa	10	266	133
5 000 tapahtumaa	50	1 330	485
10 000 tapahtumaa	100	2 660	740
100 000 tapahtumaa	1 000	26 600	7 400
500 000 tapahtumaa	5 000	133 000	37 000

Credit-korttien tapauksessa Host Card Emulationin kustannukset ovat merkittävästi korkeammat kuin Debit-korteilla. Tämä johtuu suoraan maksukorttityyppien erilaisesta kustannusrakenteesta maksukortin tarjoajan puolelta. HCE:n voidaan huomata olevan molemmissa hintaluokissa ikään kuin väliinputoajan roolissa, sillä se ei menesty muita paremmin millään ostomäärillä. Täytyy kuitenkin muistaa, ettei se automaattisesti tarkoita ratkaisun olevan muita huonompi kaikissa tilanteissa.

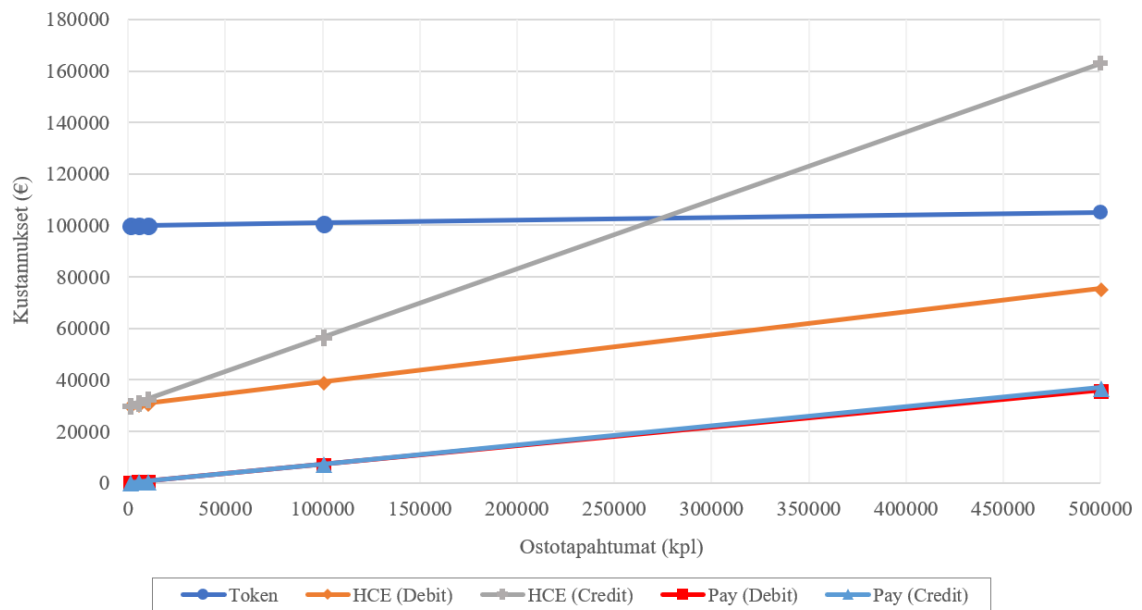
Token-pohjaisessa järjestelmässä käyttökustannukset puolestaan eivät ole riippuvaisia maksukortin tyylistä, joten kustannukset ovat samat kuin Debit-kortilla. Myös Pay-palveluiden kustannukset ovat käytetyn kustannusarvion mukaisesti lähellä aiemmin esiteltyjä Debit-korttien arvoja, mutta todellisuudessa nämäkin kustannukset riippuvat valittavasta palvelusta.

On kuitenkin myös syytä huomioda, että todellisuudessa samassa maksujärjestelmässä voi olla käytössä sekä Debit- että Credit-kortteja. Tällöin käyttökustannukset ovat jotakin

esitettyjen arvojen väliltä, riippuen suhteesta, jolla asiakkaat käyttävät Debit- ja Credit-kortteja. Seuraavassa osiossa on kehitys- ja käyttökustannusten yhteenveto sekä kustannusten kuvaaja, jonka avulla niitä on helpompi vertailla toisiinsa.

4.2.1 Kustannuksien yhteenveto

Vaihtelevat kehityskustannukset asettavat ratkaisut erilaiseen asemaan riippuen ostotapahtumien määrästä. Korkeiden kehityskustannusten vuoksi esimerkiksi token-pohjanen järjestelmä ei ole järkevä vaihtoehto pienille myyntimäärille, ellei kyseisestä ratkaisusta esimerkiksi tarpeellisten ominaisuuksien muodossa koidu merkittävää hyötyä verrattuna muihin. Vähäisten myyntimäärien kohdalla ulkopuolinen Pay-palvelu osoittautuu paremmaksi ratkaisuksi, mikäli on valmis luottamaan mobiilimaksuliiketoimintansa hallinnan ulkopuoliselle taholle. Host Card Emulation tarjoaa näiden kahden väliltä olevan ratkaisun, jossa sovellus on edelleen omassa hallinnassa. Seuraavaan kuvaajaan on yhdistetty kehitys- ja käyttökustannusten vaikutukset vertailtavista ratkaisuvaihtoehdoista.



Kuva 9. Eri ratkaisujen kokonaiskustannusarviot.

Pelkkiä Credit-kortteja hyödyntävän HCE-ratkaisun voidaan kuvasta 9 huomata nousevan melko nopeasti kiistatta kaikkein kalleimmaksi ratkaisuksi. Molempien tyyppisiä kortteja tukevan ratkaisun kustannukset leikkaavat token-järjestelmän kustannukset hiukan myöhempanä riippuen käytössä olevien korttien suhteesta. Viimeistään tämä tapahtuu 864 000 oston kohdalla, jossa pelkkiä Debit-kortteja tukevan Host Card Emulation järjestelmän kustannukset kohtaavat token-pohjaisen järjestelmän kustannukset.

Pay-palveluiden kustannukset kohtaavat token-järjestelmän kustannukset noin 1,6 miljoonan ostotapahtuman eli myynnillisesti 46 miljoonan euron kohdalla. Tämän rajapyykin jälkeen voidaan todeta token-pohjaisen järjestelmän olevan ehdottomasti paras vaihtoehto,

sillä tällöin käytössä on sekä halvimmat kustannukset että paras räätälöitävyys ja koko järjestelmän hallinta. Ratkaisujen räätälöitävyydestä kerrotaan lisää seuraavassa alaluvussa. Sen lisäksi vertaillaan ratkaisuja eri ominaisuuksien avulla.

4.3 Räätälöitävyys

Eri ratkaisuihin on mahdollista valita erilaisia palvelua mukauttavia ominaisuuksia. Ominaisuuksien tärkeys riippuu täysin käyttötarkoituksesta, johon palvelun odotetaan sopivan. Osa ominaisuuksista saattaa osoittautua välttämättömäksi osaksi liiketoimintaa, jolloin niiden puute voi rajata harkittavia vaihtoehtoja. Tästä syystä on olennaista vertailla myös mahdollisia ominaisuuksia kustannusten ohella.

Tässä työssä kaikkia ominaisuuksia vertaillaan teknisestä näkökulmasta. Tällöin vertailu ottaa enemmän kantaa siihen, mikä on mahdollista ja mikä ei jättäen ominaisuuden arvon ja tarpeen puntaroimisen lukijalle, joka tuntee millaiseen tilanteeseen mobiilimaksuratkaisua ollaan suunnittelemassa ja osaa täten antaa eri ominaisuuksille niille kuuluvan arvon osana kokonaisuutta.

4.3.1 Offline-käyttö

Offline-käytöllä tarkoitetaan mobiililaitteen mahdollisuuksia toimia suunnitellulla tavalla ilman internet-yhteyttä. Tämä voi olla tärkeä ominaisuus syrjäseuduilla, missä verkkoyhteydet voivat olla heikompia kuin kaupungeissa, tai niiden käytössä voi esiintyä enemmän katkoksia ja epävarmuutta. Mikäli maksaminen on mahdollista myös ilman verkkoyhteyttä, ei käyttäjien tarvitse huolehtia verkkoyhteyden katkeamisesta maksuhetkellä tai verkon käyttämisestä mahdollisesti koituvista kustannuksista. Jokaiseen esitettyyn ratkaisuvaihtoehtoon on kuitenkin mahdollista sisällyttää ilman verkkoyhteyttä tapahtuva maksaminen, mutta se saattaa vaatia lisäkehitystä tai tietynlaisen sovellusarkkitehtuurin valintaa. Useimmat sovellukset kuitenkin hyödyntävät internet-yhteyttä vähintään rekisteröitymisvaiheessa tai uuden maksukortin lisäämisessä.

Token-pohjaisessa järjestelmässä tämä ominaisuus vaatii suuria offline-käyttöä tukevia ratkaisuja, jotka on syytä huomioida alusta lähtien tai joiden lisääminen jälkikäteen voi aiheuttaa paljon muutoksia sovellusarkkitehtuuriin ja täten merkittäviä kustannuksia. Offline-käyttö voidaan toteuttaa joko lataamalla kertakäyttöinen token laitteelle silloin, kun verkkoyhteys on käytettävissä tai hyödyntämällä kiinteää tokenia ja kassapäätteen verkkoyhteyttä maksun suorittamiseen, kuten luvun 3.1 kuvassa 4 esitettiin.

Ennalta ladattava kertakäyttöinen token mahdollistaa yhden maksun suorittamisen, jonka jälkeen käyttäjän täytyy päästä lataamaan uusi token ennen seuraavaa maksua. Kiinteän tokenin käyttäminen on puolestaan turvattomampaa, sillä mikäli token onnistutaan varastamaan, on maksujen suorittaminen mahdollista ilman käyttäjän suostumusta. Kassapäätteen verkkoyhteyttä hyödyntävissä ratkaisuissa ongelmaksi voi koitua myös kassapäätteelle suoritettavat mahdollisesti suuret päivitykset, jotka voivat osoittautua kalliiksi.

Täyttä offline-tukea tavoiteltaessa Host Card Emulation on esitellyistä ratkaisuista helppoin, sillä kyseinen teknologiavalinta perustuu mobiililaitteen NFC-yhteyden käyttämiseen internet-yhteyden sijaan. Tällöin mobiilimaksamisen suorittamiseen laitteelta ei vaadita, ainakaan maksun yhteydessä, pääsyä internetiin, sillä tätä maksutapaa käyttäessä kassapäätte huolehtii maksun varmentamisesta ja suorittamisesta, kuten tavallista lähimaksua käytettäessä. Maksukortin tiedot puolestaan voidaan säilyttää salattuna tallessa mobiililaitteen muistissa tai Secure Elementissä, jotta niitä ei tarvitse hakea uudelleen maksua varten.

Ulkopuolisten Pay-palveluiden tapauksessa tilanne on monimutkaisempi. Monet tarjolla olevista palveluista mahdollistavat offline-maksamisen, mutta eivät kuitenkaan kaikki. Tämä riippuu siitä, miten kyseinen palvelu on toteutettu. Palveluissa voi olla myös tiettyjä rajoituksia esimerkiksi siihen, kuinka monta maksua voidaan suorittaa ennen käyntiä internetissä. Tällaisiin rajoituksiin ei välttämättä itse voi vaikuttaa. Offline-käyttö saattaa vaatia suuria muutoksia palvelun toimintaan, joten sen lisäämisen pyytäminen ei välttämättä tuota tulosta, tai sen kustannukset voivat osoittautua suuriksi. Tästäkin syystä on tärkeää punnita tarvittavat ominaisuudet ennen sitoutumista johonkin palveluun.

4.3.2 Maksupaikat

Olennainen osa teknologiaa valittaessa on, missä järjestelmän mobiilimaksujen halutaan olevan mahdollisia suorittaa. Tämä vaikuttaa myös siihen, minkälaisia ihmisiä järjestelmälle toivotaan käyttäjiksi sekä siihen, kuinka yleishyödyllinen mobiilimaksamisen sovelluksesta tulee. Mikäli sovellus toimii vain yhden tyyppisissä toimipisteissä, voi käyttäjän kynnys palvelun käyttöönottamiseksi olla suurempi kuin tilanteessa, jossa palvelu on käytettävissä useimmissa hänen suosimissaan liikkeissä.

Token-pohjainen ratkaisu vaatii kassapäätteiltä tukea, mikä hankaloittaa järjestelmän levittämistä ja soveltamista omien maksupaikkojen ulkopuolelle. Tällöin tämän ratkaisun käyttäminen on helposti rajattu vain tiettyyn liikkeeseen tai ketjuun. Tämä ei kuitenkaan ole ongelma, mikäli se on juuri sitä, mitä järjestelmältä toivotaan ja mihin se on suunniteltu. Käyttäjän kynnys voi olla suurempi asentaa tällainen sovellus, erityisesti mikäli omassa mobiililaitteessa on vähän tallennustilaa.

HCE-ratkaisu puolestaan toimii automaattisesti kaikissa niissä kohteissa, missä kyseisen maksukortin lähimaksukin toimii. Mikäli käytössä on yleiskäyttöinen korttityyppi, kuten esimerkiksi Visan tai Mastercardin Debit- tai Credit-kortti, toimii tämä ratkaisu lähes kaikissa kohteissa Suomessa ja lisäksi myös ulkomailla. Täysin omaa korttityyppiä hyödyntävällä ratkaisulla saattaa kuitenkin olla vastaava ongelma kuin token-pohjaisella järjestelmällä, jolloin kehitetty ratkaisu toimii vain omissa kohteissa.

Maailmanlaajusten ulkopuolisten mobiilimaksupalveluiden, kuten Apple Payn, hyödyntämisessä yksi merkittävimmistä vahvuuksista onkin se, että niitä voi käyttää monissa kohteissa myös Suomen ulkopuolella. Suuret palvelut houkuttelevat kauppiaita helpommin ottamaan kyseisen maksutavan käyttöön omassa liikkeessään, mikä auttaa laajentamaan verkostoa, jossa kyseisellä palvelulla voidaan maksaa. Pienillä palveluilla tätä etua ei ole, mutta

tilanne saattaa silti olla parempi kuin oman token-pohjaisen järjestelmän kanssa. Lisäksi nämä ulkopuoliset palveluntarjoajat tarjoavat usein kauppiaille mahdollisimman helppoa ja halpoja tapoja ottaa käyttöön tällainen maksutapa, mikä saattaa osaltaan rohkaista käyttöönotossa.

4.3.3 Laitetuki

Laitetuki määrittää, millä mobiililaitteilla kyseinen palvelu toimii. Tällöin se myös suoraan rajoittaa, keiden käyttäjien on mahdollista hyödyntää kyseistä palvelua, sillä he voivat käyttää palvelua vain, mikäli se toimii heidän laitteillaan. Mitä useammalla laitteella palvelua on mahdollista käyttää, sitä suurempi on potentiaalinen käyttäjäkunta. Kaikkia maailman mobiililaitteita on kuitenkin käytännössä mahdotonta tukea. Tästä syystä on tärkeää miettiä, mitä laitteita tuetaan ja mitä ei. Tätä rajausta miettiessä kannattaa määrittää tavoiteltu kohderyhmä mahdollisimman tarkasti ja tämän avulla selvittää toivotut ominaisuudet järjestelmälle.

Tokeneiden hyödyntämiseen pohjautuva palvelu tarjoaa tässä suhteessa ratkaisuihin laajimman potentiaalin. Järjestelmästä on mahdollista kehittää kaikille haluamilleen alustoille oma sovellusversio, sillä siihen ei automaattisesti sisälly merkittäviä laitteita rajaavia vaatimuksia, kuten tiettyä käyttöjärjestelmää tai pakollista NFC-yhteyttä. Tämä mahdollistaakin esitellyistä ratkaisuksista laajimman laitetuken, johon on lisäksi vertailluista teknologioista helpointa itse vaikuttaa.

Applen iPhonejen NFC-piiriin käyttöä koskevat rajoitukset rajaavat Host Card Emulationin sekä vastaavat maksuratkaisut pois käytöstä kyseisellä alustalla. Tämä on merkittävä takaisku, mikäli toiveissa on hyödyntää toiminnaltaan vastaavaa ratkaisua molemmilla suurilla alustoilla. Lisäksi HCE vaatii vähintään Androidin versiota 4.4, jolloin tätä vanhemmat versiot jäävät automaattisesti tuen ulkopuolelle. Haitta ei kuitenkaan ole kovin suuri, sillä tuota versiota vanhempien laitteiden osuus on pieni. Suurempi rajaava tekijä on pakollinen NFC-piiri, sillä ilman sitä ei luonnollisesti voida suorittaa NFC-tukea vaativia lähimaksuja.

Myös monilla ulkopuolisilla Pay-palveluilla on rajoituksia siitä, millä laitteilla palvelua on mahdollista käyttää. Palvelu voi olla esimerkiksi sidottu tiettyyn käyttöjärjestelmään tai tietyn laitevalmistajan laitteisiin. Tällaisessa tilanteessa asialle ei ole käytännössä mitään tehtävissä yksittäisen palvelun kohdalla, mutta ratkaisuna voi toimia useamman eri palvelun yhtäaikaista käyttöönotto, jotta kaikkia haluttuja mobiililaitteita voidaan tukea. Kuitenkin on olemassa myös useammalle alustalle valmiiksi sovitettuja ratkaisuja, joita voi harkita, mikäli tavoitteina on useamman alustan tukeminen.

4.3.4 Käyttäjien seuranta

Käyttäjien seuranta tarkoittaa datan keräämistä käyttäjien toiminnasta ja siitä, kuinka he esimerkiksi käyttävät sovellusta. Tämän datan avulla on mahdollista arvioida sekä

kehittää omaa liiketoimintaa ja palveluita soveltumaan paremmin kuluttajien tarpeisiin sekä kohdentaa mainontaa kuluttajasta tehdyn analyysin perusteella. Se, mitä dataa ja kuinka paljon sitä kerätään sekä miten sitä hyödynnetään, riippuu täysin palveluntarjoajasta. Data voi olla äärimmäisen arvokasta tietoa, jota kannattaa kuitenkin kerätä hienovaraisesti, sillä kuluttajat eivät pidä liian laajasta seurannasta.

Lisäksi on syytä huomioida Euroopan unionin uusi tietosuoja-asetus *GDPR*. Asetus tulee voimaan 25.5.2018, mutta se on vaatinut lukuisia järjestelmäpäivityksiä jo ennen kyseistä määräaika, jotta vaatimukset täyttyvät asetuksen tullessa voimaan. Tällöin EU-kansalaisilla tulee olla oikeus tarkistaa kaikki itsestään tallennetut tiedot sekä saada tietoa siitä, kuinka niitä on kerätty tai käsitelty. Tämä saattaa rajoittaa kerättävien tietojen määrää, mikäli tiedot ovat yhdistettävissä henkilöön. [61]

Tässä työssä kyseistä ominaisuutta kuitenkin vertaillaan teknisestä lähtökohdasta, ottamatta kantaa siihen, mitä tietoa missäkin tilanteessa on järkevää kerätä tai tallentaa. Tällöin lukijan on helpompi vertailla sitä, mikä on mahdollista milläkin ratkaisulla. Tämän jälkeen on mahdollista punnita, mikä tieto on tärkeää ja kuinka uusi tietosuoja-asetus vaatimuksineen täytetään.

Täysin omana järjestelmänä token-pohjainen ratkaisu tarjoaa suurimmat mahdollisuudet datan keräämiseen. Tällaisella palvelulla voidaan kerätä dataa mobiilisovelluksen lisäksi myös kassapäätteistä ja palvelimilta. Tällöin on tarvittaessa mahdollista kerätä mobiililaitteelta tietoa siitä, kuka ostaa, mistä ostaa ja milloin ostaa sekä yhdistää tietoihin kassapäätteeltä saatavat tiedot siitä, mitä tuotteita hän on ostanut ja mihin hintaan. Kun nämä tiedot yhdistetään palvelimella, voidaan saada hyvinkin tarkka kuva käyttäjien toiminnasta, kulutustottumuksista ja siitä, mistä tuotteista he ovat kiinnostuneita. Tällaisessa järjestelmässä on kuitenkin mahdollista myös rajoittaa datan keräämistä niihin asioihin, joita todella halutaan seurata ilman ylimääräisen tai arkaluontoisen tiedon keräämistä.

Myös Host Card Emulation tarjoaa mahdollisuuksia käyttäjien toiminnan seuraamiseen, vaikkei kuitenkaan yhtä laajasti kuin token-pohjainen järjestelmä. Tällöin ei ole yhtä helppoa tai kaikissa tilanteissa mahdollistakaan saada kassapäätteeltä tietoja. Käytössä on kuitenkin kaikki mobiililaitteelta itseltään kerättävät tiedot, mutta ilman tarkkoja tuotetietoja on vaikeampi analysoida kuluttajan tottumuksia yhtä tarkasti.

Ulkopuoliset palveluntarjoajat eivät puolestaan yleensä mahdollista käyttäjien seuraamista ollenkaan. Useilla palveluilla kuitenkin lienee vastaavan kaltaista seuranta käytössään, mutta ne eivät ole halukkaita jakamaan tätä keräämäänsä dataa. Tällä datan keräämisellä nämä palvelut saattavat kompensoida muutoin palvelun kustannuksia, sillä tällöin käyttäjästä on tullut ikään kuin tuote, josta palveluntarjoaja saa tuloja hyödyntämällä hänen tietojaan ja mahdollisesti myymällä niitä eteenpäin.

4.3.5 Ominaisuuksien yhteenveto

Seuraavaksi on yllä esiteltyjen ominaisuuksien taulukkoon 3 tiivistetty yhteenveto. Tämä mahdollistaa helpomman vertailun jo nopealla silmäyksellä. Taulukon tähtien asteikko

on yhdestä viiteen tähteä. Arvosana yksi tarkoittaa sitä, että ominaisuus on joko huonosti tuettu tai se ei ole saatavilla ollenkaan. Viisi puolestaan tarkoittaa erinomaista tai erittäin hyvää tukea. Joissakin tapauksissa, erityisesti ulkopuolisia Pay-palveluita ajatellen, on vaikeaa arvioida ominaisuuden todellista tilaa tai sen toteutettavuutta. Tämä on esitetty kysymysmerkillä tähtien perässä. Tällöin todellinen arvo riippuu todella paljon siitä, mitä palvelua halutaan vertailla muihin ratkaisuihin. Tähtien lisäksi taulukkoon on koottu lyhyet kommentit kyseisestä ominaisuudesta.

Taulukko 3. Ominaisuuksien vertailu eri ratkaisujen välillä. Tähtien asteikko on yhdestä viiteen tähteä.

	Token	HCE	Ulkopuolinen
Offline-käyttö	*** Mahdollista, mutta saattaa olla työlästä.	***** Automaattisesti tuettu.	***? Saattaa olla valmiina käytössä, mutta riippuu täysin palveluntarjoajasta.
Maksupaikat	* Usein vain omat kohteet. Vaikea levittää laajasti.	***** Toimii kaikkialla, missä tavallinen lähimaksu kyseisellä kortilla toimii.	***** Usein tuettu monissa paikoissa myös ulkomailla, muttei aivan kaikkialla. Kuitenkin yleensä tarjotaan helppoja tapoja ottaa käyttöön.
Laitetuki	***** Mahdollista kehittää mille tahansa haluamalleen järjestelmälle.	** Käytännössä vain Android 4.4 ja sitä uudemmat NFC-yhteensopivat Android-mobiililaitteet.	***? Riippuu täysin palvelusta.
Käyttäjien seuranta	***** Mahdollistaa yksityiskohtaisen seurannan, johon voidaan yhdistää monipuolista tietoa.	*** Voidaan kerätä tietoa, mutta vain yksipuoleisesti.	* Ei mahdollista.

Tähtien yhteenlaskettu summa ei kuitenkaan suoraan kerro, mikä ratkaisusta olisi kokonaisuutena yksiselitteisesti paras. Tämä johtuu siitä, että eri ominaisuuksilla on erilainen arvo jokaisessa käyttötärpeessä ja siinä, miten järjestelmää on suunniteltu käytettävän. Tähdet yhdessä kommenttien kanssa kuitenkin helpottavat kyseisen ominaisuuden vertailua eri teknologiaratkaisujen kesken.

Eteen on mahdollista tulla myös tilanteita, joissa jollakin ominaisuudella ei ole mitään arvoa, vaikka se olisi luokiteltu viidellä tähdellä. Esimerkiksi mikäli ei haluta seurata käyttäjiä, ei token-pohjaisen järjestelmän viidellä tähdellä ole mitään arvoa, eikä vastaavasti ulkopuolisen Pay-palvelun yhdellä tähdellä mitään haittaa. Tällaiset tilanteet on syytä huomioida alusta alkaen eri vaihtoehtoja punnittaessa, jotta ne eivät pääse vääristämään tuloksia todellisen tarpeen näkökulmasta.

4.4 Mobiilimaksamisen tulevaisuus

Vaikka mennyt ei aina olekaan tae tulevasta, voidaan kuitenkin olettaa, että mobiilimaksaminen jatkaa kasvuaan. Kasvun myötä nykyiset ratkaisut saattavat kehittyä tai muuttaa muotoaan. Lisäksi Suomeen vaikuttavat etenkin myös muissa Pohjoismaissa hyödynnetyt ratkaisut. Erityisesti Ruotsissa ja Tanskassa mobiilimaksamisella on paljon suurempi osuus kuluttajia, jotka käyttävät sitä vähintään kuukausittain. Tämän lisäksi Ruotsissa odotetaan jo käteisen ja maksukorttien katoamista mobiilimaksamisen tieltä. [54]

Suuret kiinalaiset ratkaisut WeChat Pay ja AliPay ovat maailmanlaajuisesti merkittäviä maksupalveluita, jotka tulevat varmasti lähitulevaisuudessa vaikuttamaan mobiilimaksamisliiketoimintaan myös Suomessa. Kyseessä on kaksi maailman suurinta mobiilimaksujärjestelmää. WeChat Pay:lla oli yhteensä peräti 600 miljoonaa ja AliPay:lla 400 miljoonaa käyttäjää elokuussa vuonna 2017 [62]. Nämä luvut jättävät toistaiseksi kaikki muut mobiilimaksupalvelut kauas taakseen. Vertailun vuoksi esimerkiksi Apple Pay:lla on 87 miljoonaa ja Google Pay:lla 24 miljoonaa käyttäjää [62].

Suurelkan palvelut eivät kuitenkaan estä muiden palvelujen kilpailua ja osallistumista samaan liiketoimintaan. Tämä johtaa tilanteeseen, jossa käyttäjillä voi olla käytössään useita eri mobiilimaksupalveluita yhtä aikaa. Tällöin he valitsevat ja käyttävät tilanteeseen parhaiten sopivaa palvelua maksun suorittamiseen.

Lisäksi entisestään kasvava markkinaosuus tarjoaa myös lukuisia uusia mahdollisuuksia. Tällöin alalla ei ole pelkästään vakiintuneita standardeja ja toimijoita, jotka vaikeuttaisivat uusien palveluiden kehittämistä. Nykyinen tilanne mahdollistaa toistaiseksi helpomman kilpailun eri palveluiden välillä ja tarjoaa myös täysin uusille yrityksille tilaa kehittää uudenlaisia ratkaisuja. Standardien puuttuminen kuitenkin myös hidastaa mobiilimaksamisen yleistymistä ja laajaa käyttöönottoa kuluttajien keskuudessa Suomessa.

Jotkin mobiilimaksupalvelut, kuten esimerkiksi Apple Pay, ovat levittäytymässä perinteisten kauppohen lisäksi myös uusiin käyttökohteisiin, kuten erilaisiin verkkokauppoihin ja mobiilisovelluksiin [32]. Verkkokauppoihin mobiilimaksaminen tuo uuden maksutavan perinteisten tapojen ohjelle. Mobiilisovelluksissa tämä ominaisuus puolestaan helpottaa

maksamista, sillä maksutietoja ei tarvitse syöttää jokaiselle sovellukselle erikseen, vaan maksaminen voidaan ohjata suoraan käytössä olevalle mobiilimaksupalvelulle. Nämä ominaisuudet eivät kuitenkaan vielä ole yleisiä kaikkien mobiilimaksupalveluiden keskuudessa, mutta monet palveluntarjoajat tulevat lähitulevaisuudessa todennäköisesti seuraamaan Applen esimerkkiä ja lisäämään vastaavia ominaisuuksia omiin palveluihinsa.

Erilaisten älypuhelimien ja tablet-laitteiden lisäksi myös muut kehittyvät mobiililaitteet tarjoavat lisäpotentiaalia mobiilimaksamisen hyödyntämiseen. Tästä hyvä esimerkki on älykellojen hyödyntäminen mobiilimaksamisessa, kuten Apple Pay:n käyttäminen Apple Watch -älykellolla [32]. Tällöin maksutilanteessa kuluttajan ei tarvitse kassalla kaivaa taskusta erillistä mobiililaitetta, vaan maksun suorittamiseen riittää ranteessa olevan älykellon näyttäminen kassapäätteelle.

5. YHTEENVETO

Tässä diplomityössä esiteltiin ja vertailtiin erilaisia mobiilimaksamisen ratkaisuja. Työ aloitettiin erilaisten maksamiskäytäntöjen ja mobiilimaksamisen yleisellä läpikäymisellä, jonka jälkeen esiteltiin eri ratkaisujen tarkempia tietoja. Lopuksi näitä eri ratkaisuja vertailtiin keskenään tarjoten pohjaa tietojen soveltamiseen omasta näkökulmasta suuntautuvaan vertailuun.

Mobiilimaksamisella tarkoitetaan maksun suorittamista, jossa vähintään yksi osasuoritus on toteutettu mobiililaitteella. Mobiilimaksaminen voidaan toteuttaa muutamilla erilaisilla tavoilla. Suomessa käytössä olevat mobiilimaksamisen ratkaisut voidaan karkeasti jakaa kolmeen erillaiseen lähestymistapaan. Nämä tavat soveltuvat erilaisiin tilanteisiin eri tavoin, sillä jokaisella valinnalla on omat hyvät ja huonot puolensa.

Ensimmäisenä esitelty tapa on toteuttaa oma maksujärjestelmä, jossa maksuja voidaan käsitellä yksilöllisillä tunnisteilla eli tokeneilla. Tämä mahdollistaa täydellisesti omiin tarpeisiin sovitettun palvelun. Maksut käsitellään erillisellä palvelimella, jonne maksujen tiedot välitetään internet-yhteyden avulla. Kokonaisen järjestelmän kehittäminen ja ylläpito voi kuitenkin osoittautua työlääksi, vaikka se tarjoaakin monia etuja verrattuna muihin ratkaisuihin.

Toinen tapa on hyödyntää monista mobiililaitteista löytyvää NFC-piiriä sekä useimmista maksupäätteistä löytyvää lähimaksuominaisuutta. Tätä kutsutaan Host Card Emulationiksi, jolloin mobiililaitte emuloi olemassa olevan maksukortin ja vastaa maksupäätteen kutsuihin samalla tavalla kuin tavallinen lähimaksukortti tekisi. Tämä ratkaisu ei edellytä uuden järjestelmän kehittämistä, vaan se voidaan ottaa käyttöön kaikkialla, missä kyseisen maksukortin lähimaksaminen on mahdollista. HCE on kuitenkin käytännössä mahdollinen ainoastaan Android-käyttöjärjestelmällä toimivissa mobiililaitteissa, minkä lisäksi se edellyttää pakollista NFC-tukea.

Kolmas tapa on luottaa mobiilimaksuratkaisunsa ulkopuolisen palveluntarjoajan käsiin. Tämä on matalan kynnyksen ratkaisu, sillä tällöin ei ole tarvetta itse kehittää uusia järjestelmiä tai mobiilisovelluksia. Tästä kuitenkin aiheutuu omat haasteensa, sillä palvelu ei ole omassa hallinnassa eikä räätälöitävissä omiin tarpeisiin. Kevyt käyttöönotto kuitenkin tarjoaa tälle ratkaisulle suurimman potentiaalin kasvaa myös pienten toimijoiden keskuudessa. Lisäksi suuret monikansalliset palvelut tarjoavat mahdollisuuden käyttää samaa ratkaisua Suomen lisäksi myös ulkomailla.

Näin ollen ei ole yksiselitteistä vastausta siihen, mikä esitellyistä ratkaisuista on paras, vaan valintaa on syytä puntaroida omien tarpeiden, resurssien ja businesslogiikan mukaan. Lisäksi mobiilimaksamisen ollessa vielä verrattain uusi teknologia, tulevat sen käyttö ja

mahdollisuudet muuttumaan vielä lähitulevaisuudessa. Tästä huolimatta työssä esiteltyt ratkaisut todennäköisesti tulevat pitämään paikkansa myös tulevaisuudessa.

Työssä käytiin läpi lähinnä Suomessa käytössä olevia mobiilimaksamisen ratkaisuja. Työtä voisi laajentaa käsittelemällä tämän lisäksi myös ulkomailla käytössä olevia ratkaisuja, niiden ominaispiirteitä sekä vaikutuksia globaaliin mobiilimaksamisen liiketoimintaan. Tämän lisäksi toinen suuri käsiteltävä asia olisi erilaisten mobiilimaksamisen ratkaisujen esittely palvelimien ja taustajärjestelmien osalta sekä perehtyminen erilaisten ratkaisujen tietoturvaan. Lisäksi ratkaisuja olisi mahdollista käsitellä teknisen toteutuskeskeisen lähestymistavan lisäksi myös käyttäjäkokemuksen kautta.

VIITTEET

- [1] statista.com. Total revenue of global mobile payment market from 2015 to 2019 (in billion U.S. dollars). [WWW]. [Viitattu 9.11.2017]. Saatavissa: <https://www.statista.com/statistics/226530/mobile-payment-transaction-volume-forecast/>.
- [2] eatech.fi. Eatech toteutti Nesteen mobiilimaksun. [WWW]. [Viitattu 9.11.2017]. Saatavissa: <https://www.eatech.fi/eatech-toteutti-nesteen-mobiilimaksun/>.
- [3] abcasemat.fi. Mobiilitankkaus. [WWW]. [Viitattu 9.11.2017]. Saatavissa: <https://www.abcasemat.fi/fi/polttoaineet/mobiilitankkaus>.
- [4] developer.android.com. Host-based Card Emulation. [WWW]. [Viitattu 5.6.2017]. Saatavissa: <https://developer.android.com/guide/topics/connectivity/nfc/hce.html>.
- [5] netmarketshare.com. Mobile/Tablet Operating System Market Share, August 2017. [WWW]. [Viitattu 20.9.2017]. Saatavissa: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1>.
- [6] Visa. Luottokunta ja Visa kontaktittoman mobiilimaksamisen pioneereina Suomessa , lehdistötiedote, 22.10.2009. Saatavissa: <http://mb.cision.com/Public/MigratedWpy/82030/700150/9945d4264cdd5523.pdf>.
- [7] eurojatalous.fi. Päivittäistavaraostojen tavallisin maksutapa. [WWW]. [Viitattu 27.9.2017]. Saatavissa: <http://www.eurojatalous.fi/fi/kuviot/graafi/paivittaistavaraostojen-tavallisin-maksutapa/>.
- [8] yle.fi. Maksupäätteiden kovat kulut ajavat yrittäjän siirtymään käteiskauppaan. [WWW]. [Viitattu 11.10.2017]. Saatavissa: <https://yle.fi/uutiset/3-6939595>.
- [9] kauppalehti.fi. Kortilla maksaminen käy kalliimmaksi kauppiaille. [WWW]. [Viitattu 21.2.2018]. Saatavissa: <https://www.kauppalehti.fi/uutiset/kortilla-maksaminen-kay-kalliimmaksi-kauppiaille/GqAibrB7>.
- [10] Kunelius, J. Mitä skimmaus on?, opinnäytetyö, 2017. Saatavissa: <https://www.theseus.fi/handle/10024/126828>.
- [11] Kokkola, T. The Payment System - Payments, Securities and Derivatives, and the Role of the Eurosystem. ISBN:978-92-899-0633-3. Saatavissa: <https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf>.

-
- [12] Tuominen, T. Mobiili lähimaksaminen - nykykäyttö ja tulevaisuus. Liikenne- ja viestintäministeriön julkaisuja 22/2003. Saatavilla: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78449/1_22_2003.pdf?sequence=1.
- [13] vertaaensin.fi. Prepaid-luottokortti – mikä se on?. [WWW]. [Viitattu 9.11.2017]. Saatavissa: <https://www.vertaaensin.fi/blog/prepaid-luottokortti>.
- [14] Pako, I. Lähimaksaminen, opinnäytetyö, 2014. Saatavissa: <http://theseus56-kk.lib.helsinki.fi/handle/10024/71349>.
- [15] nordea.fi. Lähimaksaminen. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/kortit/lahimaksaminen.html>.
- [16] poppankki.fi. Mitä Lähimaksaminen on?. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://www.poppankki.fi/henkiloasiakkaat/paivittaiset-raha-asiat/kortit/n%C3%A4in-l%C3%A4himaksat>.
- [17] s-pankki.fi. Lähimaksaminen – helppoa, turvallista ja nopeaa. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://www.s-pankki.fi/fi/arjen-raha-asiat/s-etukortti-visa/lahimaksaminen/>.
- [18] uusi.op.fi. Lähimaksaminen – nopeaa ja turvallista. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://uusi.op.fi/henkiloasiakkaat/paivittaiset/maksaminen/lahimaksaminen-nopeaa-ja-turvallista>.
- [19] danskebank.fi. Lähimaksaminen. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://danskebank.fi/fi-fi/Henkiloasiakkaat/Paivittaiset-raha-asiat/Kortit/Pages/Lahimaksaminen.aspx>.
- [20] visa.fi. Lähimaksaminen – Yleisimpiä kysymyksiä. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://www.visa.fi/fi/maksa-visalla/lahimaksaminen/yleisimpia-kysymyksia>.
- [21] nets.eu. Lähimaksaminen. [WWW]. [Viitattu 23.11.2017]. Saatavissa: <https://www.nets.eu/fi/payments/korttimaksut-myyمالassa/lisaarvopalvelut/lahimaksaminen/>.
- [22] Kokko, T. Lähimaksaminen ja sen turvallisuus, opinnäytetyö, 2016. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/108736/Kokko_Taru.pdf?sequence=1.
- [23] forbes.fi. See How This Android App Clones Contactless Credit Cards In Seconds. [WWW]. [Viitattu 9.11.2017]. Saatavissa: <https://www.forbes.com/sites/forbes/2017/11/09/android-app-clones-contactless-credit-cards-in-seconds/#1>.

[//www.forbes.com/sites/thomasbrewster/2015/02/18/android-app-clones-cards/#6de5bcf4db39](http://www.forbes.com/sites/thomasbrewster/2015/02/18/android-app-clones-cards/#6de5bcf4db39).

- [24] Karnouskos, S., Mobile Payment: A Journey Through Existing Procedures And Standardization Initiatives. IEEE Communications Surveys & Tutorials, Fourth Quarter, VOL. 6, NO. 4, 2004. Available: https://www.researchgate.net/profile/Stamatis_Karnouskos/publication/224085138_Mobile_payment_A_journey_through_existing_procedures_and_standardization_initiatives/links/0046353626a53ee797000000.pdf.
- [25] kauppalehti.fi. Näin maksaminen muuttuu - maksukortti katoaa, käteinen jää historiaan. [WWW]. [Viitattu 29.9.2017]. Saatavissa: <https://www.kauppalehti.fi/uutiset/nain-maksaminen-muuttuu---maksukortti-katoaa--kateinen/xGRmPdts>.
- [26] Klaper, J. Tietoturvan huomioiminen maksujärjestelmässä, diplomityö, 2016. Saatavissa: <https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/23928/Klaper.pdf?sequence=1>.
- [27] Hautala, H. Androidin fragmentaatio - ongelmia ja ratkaisuja, diplomityö, 2015. Saatavissa: <https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/23011/hautala.pdf?sequence=1>.
- [28] opensignal.com. Android Fragmentation 2015. [WWW]. [Viitattu 14.12.2017]. Saatavissa: <https://opensignal.com/reports/2015/08/android-fragmentation/>.
- [29] developer.android.com. Dashboards. [WWW]. [Viitattu 4.6.2017]. Saatavissa: <https://developer.android.com/about/dashboards/index.html>.
- [30] developer.android.com. App Manifest. [WWW]. [Viitattu 21.12.2017]. Saatavissa: <https://developer.android.com/guide/topics/manifest/manifest-intro.html>.
- [31] developer.apple.com. iOS Device Compatibility Reference. [WWW]. [Viitattu 21.12.2017]. Saatavissa: <https://developer.apple.com/library/content/documentation/DeviceInformation/Reference/iOSDeviceCompatibility/DeviceCompatibilityMatrix/DeviceCompatibilityMatrix.html>.
- [32] apple.com. Apple Pay. [WWW]. [Viitattu 5.6.2017]. Saatavissa: <https://www.apple.com/apple-pay/>.
- [33] cultofmac.com. Apple confirms iPhone 6 NFC chip is only for Apple Pay at launch. [WWW]. [Viitattu 21.12.2017]. Saatavissa: <https://www.cultofmac.com/296093/apple-confirms-iphone-6-nfc-apple-pay/>.

-
- [34] O’Gorman, L., Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, VOL. 91, NO. 12, 2003. p. 2019-2040 Available: <http://ieeexplore.ieee.org/document/1246384/?reload=true>.
- [35] tools.ietf.org. HTTP over TLS. [WWW]. [Viitattu 18.1.2018]. Saatavissa: <https://tools.ietf.org/html/rfc2818>.
- [36] nets.eu. PCI-DSS-standardin 12 vaatimusta. [WWW]. [Viitattu 10.1.2018]. Saatavissa: <https://www.nets.eu/fi/payments/korttimaksujen-turvallisuus/PCI-standardi/pci-dss-standardin-12-vaatimusta/>.
- [37] Denso ADC. QR Code Essentials. [WWW]. [Viitattu 21.2.2018] Saatavilla: <http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D>.
- [38] vm.fi. Maksujärjestelmät. [WWW]. [Viitattu 2.11.2017]. Saatavissa: <http://vm.fi/maksujarjestelmat>.
- [39] finanssivalvonta.fi. Uusi maksupalveludirektiivi – Payment Services Directive, PSD2. [WWW]. [Viitattu 18.1.2018]. Saatavissa: <http://www.finanssivalvonta.fi/fi/Saantely/Saantelyhankkeet/PSD2/Pages/Default.aspx>.
- [40] nordea.com. EU:n uusi maksupalveludirektiivi PSD2 pian voimaan. [WWW]. [Viitattu 18.1.2018]. Saatavissa: <https://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/News-fi/2017/2017-11-21-EUn-uusi-maksupalveludirektiivi-PSD2-pian-voimaan.html>.
- [41] marmai.fi. Suurin osa kuluttajista valitsi yksityisyyden käyttökokemuksen kustannuksella. [WWW]. [Viitattu 25.1.2018]. Saatavissa: <https://www.marmai.fi/uutiset/suurin-osa-kuluttajista-valitsi-yksityisyyden-kayttokokemuksen-kustannuksella-6682691>.
- [42] pressreleases.visa.com. Visa to Enable Secure, Cloud-Based Mobile Payments. [WWW]. [Viitattu 31.1.2018]. Saatavissa: <http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1901153&highlight=HCE>.
- [43] newsroom.mastercard.com. MasterCard to Use Host Card Emulation (HCE) for NFC-Based Mobile Payments. [WWW]. [Viitattu 31.1.2018]. Saatavissa: <https://newsroom.mastercard.com/press-releases/mastercard-to-use-host-card-emulation-hce-for-nfc-based-mobile-payments/>.
- [44] developer.android.com. CardEmulation. [WWW]. [Viitattu 28.2.2018]. Saatavissa: <https://developer.android.com/reference/android/nfc/cardemulation/CardEmulation.html>.

-
- [45] International Standard. Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange . ISO/IEC 7816-4, Second edition. 2005-01-15.
- [46] <http://blog.simplytapp.com>. Host Card Emulation Series: SwipeYours - Tap Using A Card From Your Wallet. [WWW]. [Viitattu 14.3.2018]. Saatavissa: <http://blog.simplytapp.com/2014/01/host-card-emulation-series-swipeyours.html>.
- [47] handstandsam.com. Droidcon NYC – Mobile Payments using Host Card Emulation. [WWW]. [Viitattu 14.3.2018]. Saatavissa: <https://handstandsam.com/2015/09/16/droidcon-nyc-mobile-payments-using-host-card-emulation/>.
- [48] EMV. Contactless Specifications for Payment Systems, Book B, Entry Point Specification. Version 2.6. July, 2016. Available: https://www.emvco.com/wp-content/uploads/2017/05/BookB_Entry_Point_Specification_v2_6_20160809023257319.pdf.
- [49] developer.android.com. HostApuService. [WWW]. [Viitattu 28.2.2018]. Saatavissa: <https://developer.android.com/reference/android/nfc/cardemulation/HostApuService.html>.
- [50] emvlab.org. EMV tag search results [WWW]. [Viitattu 7.3.2018]. Saatavissa: <http://emvlab.org/emvtags/all/>.
- [51] developer.blackberry.com. NFC API. [WWW]. [Viitattu 17.3.2018]. Saatavissa: https://developer.blackberry.com/native/documentation/device_comm/nfc/nfc_api.html.
- [52] docs.microsoft.com. Create an NFC Smart Card app. [WWW]. [Viitattu 17.3.2018]. Saatavissa: <https://docs.microsoft.com/en-us/windows/uwp/devices-sensors/host-card-emulation>.
- [53] android.com. Android Pay. [WWW]. [Viitattu 3.6.2017]. Saatavissa: <https://www.android.com/pay/>.
- [54] yle.fi. Kännykkämaksaminen Suomessa vielä lapsenkengissä – Ruotsissa povataan jo käteisen kuolemaa. [WWW]. [Viitattu 6.4.2018]. Saatavissa: <https://yle.fi/uutiset/3-10094786>.
- [55] ts.fi. Suomalaiset vinguttavat Visaa ahkerasti [WWW]. [Viitattu 11.4.2018]. Saatavissa: <http://www.ts.fi/uutiset/kotimaa/730948/Suomalaiset+vinguttavat+Visaa+ahkerasti>.

-
- [56] yrittajat.fi. Käteinen vai kortti? Näin syntyy yrittäjälle kuluja [WWW]. [Viitattu 11.4.2018]. Saatavissa: <https://www.yrittajat.fi/uutiset/498133-kateinen-vai-kortti-nain-syntyy-yrittajalle-kuluja>.
- [57] gomedici.com. Intriguing Apple Pay Details Revealed [WWW]. [Viitattu 16.4.2018]. Saatavissa: <https://gomedici.com/intriguing-apple-pay-details-revealed/>.
- [58] digitaltrends.com. There are no transaction fees for Android Pay, which is good for us, bad for Google [WWW]. [Viitattu 18.4.2018]. Saatavissa: <https://www.digitaltrends.com/mobile/googles-unwanted-advantage-no-transaction-fees-for-android-pay/>.
- [59] sttinfo.fi. Suomen ensimmäinen kaikille pienyrityksille sopiva mobiilimaksuratkaisu julki [WWW]. [Viitattu 18.4.2018]. Saatavissa: <https://www.sttinfo.fi/tiedote/suomen-ensimmainen-kaikille-pienyrityksille-sopiva-mobiilimaksuratkaisu-julki?publisherId=55565369&releaseId=62095783>.
- [60] mobilepay.fi. MobilePay MyShop [WWW]. [Viitattu 18.4.2018]. Saatavissa: <https://www.mobilepay.fi/fi-fi/Yritykset/Pages/mobilepay-myshop.aspx>.
- [61] tietosuoja.fi. EU:n tietosuojauudistus [WWW]. [Viitattu 9.5.2018]. Saatavissa: <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html>.
- [62] statista.com. Number of users of leading mobile payment platforms worldwide as of August 2017 [WWW]. [Viitattu 9.5.2018]. Saatavissa: <https://www.statista.com/statistics/744944/mobile-payment-platforms-users/>.